HE
18.5
.A37
no.
DOT-
TSC-
UMTA-
80-37

ORT NO. UMTA-MA-06-0048-80-9

MAR 4 1981

MORGANTOWN PEOPLE MOVER
COLLISION AVOIDANCE SYSTEM DESIGN SUMMARY

Robert J. Schroder
Roy S. Washington

BOEING AEROSPACE COMPANY
Automated Transportation Systems
Seattle, Washington 98124

SEPTEMBER 1980

FINAL REPORT

DOCUMENT IS AVAILABLE TO THE PUBLIC
THROUGH THE NATIONAL TECHNICAL
INFORMATION SERVICE, SPRINGFIELD,
VIRGINIA 22161

Prepared for

U.S. DEPARTMENT OF TRANSPORTATION
URBAN MASS TRANSPORTATION ADMINISTRATION
Office of Technology Development and Deployment
Office of AGT Applications
Washington, DC 20590

NOTICE

This document is disseminated under the sponsorship of the Department of Transportation in the interest of information exchange. The United States Government assumes no liability for its contents or use thereof.

NOTICE

The United States Government does not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the object of this report.

no.
DOT-
TSC-
UMTA-
80-37

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
UMTA-MA-06-0048-80-9	PB 81-154858	

4. Title and Subtitle	5. Report Date
MORGANTOWN PEOPLE MOVER COLLISION AVOIDANCE SYSTEM DESIGN SUMMARY	September 1980
	6. Performing Organization Code DTS-723
7. Author(s) Robert J. Schroder and Roy S. Washington	8. Performing Organization Report No. DOT-TSC-UMTA-80- 37
9. Performing Organization Name and Address Boeing Aerospace Company* Automated Transportation Systems Seattle, WA 98124	10. Work Unit No. (TRAIS) UM041/R0725
	11. Contract or Grant No. DOT-TSC
12. Sponsoring Agency Name and Address U.S. Department of Transportation Urban Mass Transportation Administration Office of Technology Development and Deployment Washington, DC 20590	13. Type of Report and Period Covered Final Report
	14. Sponsoring Agency Code UTD-60

15. Supplementary Notes

* Under contract to: U.S. Department of Transportation
Research and Special Programs Administration
Transportation Systems Center, Kendall Square
Cambridge, MA 02142

16. Abstract

This report summarizes the design and development of the Collision Avoidance System (CAS) for the Morgantown People Mover - a fully automated transportation system utilizing rubber-tired vehicles operating at short headway. Identified safety and operability requirements led to a unique implementation of a proven safety concept - block occupancy control.

Problems encountered and the design solutions which evolved are discussed with emphasis upon fail-safe features. The resulting CAS design is assessed and found to be extremely safe.

Possible improvements and extensions are discussed. Shorter headway and bidirectional operation are found to be feasible.

17. Key Words	18. Distribution Statement
Collision Avoidance, Fail-safe, Headway, Presence Detection, Block Occupancy, Checked Redundancy, Disparity Detection, AGT, Safety, Morgantown	DOCUMENT IS AVAILABLE TO THE PUBLIC THROUGH THE NATIONAL TECHNICAL INFORMATION SERVICE, SPRINGFIELD, VIRGINIA 22161

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
UNCLASSIFIED	UNCLASSIFIED	168	

PREFACE

This report describes the Collision Avoidance System (CAS) design used for the current (1980 Phase II) Morgantown People Mover (MPM) system. Since the MPM system was developed in three phases, this report presents some historical data leading to the current design. This report also includes results of experience with the collision avoidance system, plans for potential system improvements, and recommendations so that future system designers can benefit from the experience gained in performing this study.

The work described in this report was sponsored by the Office of AGT Applications, Office of Technology Development and Deployment of the U.S. Department of Transportation's Urban Mass Transportation Administration. This report was monitored by U.S. Department of Transportation, Transportation Systems Center (TSC), Cambridge, Massachusetts.

The bulk of the design of the CAS was accomplished by the Bendix Corporation, Ann Arbor, Michigan. Recent improvements were designed by Boeing Aerospace Company, Seattle, Washington. Some of the early trade studies were performed by Jet Propulsion Laboratory (JPL), Pasadena, California.

METRIC CONVERSION FACTORS

Approximate Conversions to Metric Measures

Symbol	When You Know	Multiply by	To Find	Symbol
		LENGTH		
in	inches	2.5	centimeters	cm
ft	feet	30	centimeters	cm
yd	yards	0.9	meters	m
mi	miles	1.6	kilometers	km
		AREA		
in^2	square inches	6.5	square centimeters	cm^2
ft^2	square feet	0.09	square meters	m^2
yd^2	square yards	0.8	square meters	m^2
mi^2	square miles	2.6	square kilometers	km^2
	acres	0.4	hectares	ha
		MASS (weight)		
oz	ounces	28	grams	g
lb	pounds	0.45	kilograms	kg
	short tons (2000 lb)	0.9	tonnes	t
		VOLUME		
tsp	teaspoons	5	milliliters	ml
Tbsp	tablespoons	15	milliliters	ml
fl oz	fluid ounces	30	milliliters	ml
c	cups	0.24	liters	l
pt	pints	0.47	liters	l
qt	quarts	0.95	liters	l
gal	gallons	3.8	liters	l
ft^3	cubic feet	0.03	cubic meters	m^3
yd^3	cubic yards	0.76	cubic meters	m^3
		TEMPERATURE (exact)		
°f	Fahrenheit temperature	5/9 (after subtracting 32)	Celsius temperature	°c

Approximate Conversions from Metric Measures

Symbol	When You Know	Multiply by	To Find	Symbol
		LENGTH		
mm	millimeters	0.04	inches	in
cm	centimeters	0.4	inches	in
m	meters	3.3	feet	ft
m	meters	1.1	yards	yd
km	kilometers	0.6	miles	mi
		AREA		
cm^2	square centimeters	0.16	square inches	in^2
m^2	square meters	1.2	square yards	yd^2
km^2	square kilometers	0.4	square miles	mi^2
ha	hectares (10,000 m^2)	2.5	acres	
		MASS (weight)		
g	grams	0.035	ounces	oz
kg	kilograms	2.2	pounds	lb
t	tonnes (1000 kg)	1.1	short tons	
		VOLUME		
ml	milliliters	0.03	fluid ounces	fl oz
l	liters	2.1	pints	pt
l	liters	1.06	quarts	qt
l	liters	0.26	gallons	gal
m^3	cubic meters	35	cubic feet	ft^3
m^3	cubic meters	1.3	cubic yards	yd^3
		TEMPERATURE (exact)		
°c	Celsius temperature	9/5 (then add 32)	Fahrenheit temperature	°f

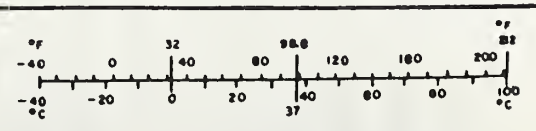


TABLE OF CONTENTS

Section		Page
1	INTRODUCTION	1
1.1	General	1
1.2	History	1
2	GENERAL SYSTEM DESCRIPTION	5
2.1	Station Control and Communications Equipment	7
2.1.1	Uplink Communications	10
2.1.2	Downlink Communications	16
2.2	Guideway Subsystem	16
2.3	Vehicles	18
2.4	Vehicle Control and Communications Subsystem (VCCS)	21
2.5	Collision Avoidance System	25
3	CAS REQUIREMENTS	28
3.1	Safety	28
3.1.1	Definitions	28
3.1.2	Safety Requirements	30
3.1.2.1	Basic Safety Requirements	30
3.1.2.2	Derived Safety Requirements	31
3.1.2.2.1	Phase II Specifications	31
3.1.2.2.2	Checked Redundancy	33
3.2	Operability	35
3.2.1	Operating Requirements	36
3.2.2	Recovery Requirements	37
3.3	Maintenance	37
4	CAS DESIGN	39
4.1	Design Concept	39
4.2	Design Technique	47
4.2.1	CAS Logic Equations	47
4.2.1.1	Block Occupancy Expressions	48
4.2.1.2	Priority Latch Expressions	49
4.2.1.3	Switch Latch Expressions	51
4.2.1.4	Safe Tone Equations	52
4.2.2	CAS Layout	57
4.2.2.1	Theoretical Considerations	57
4.2.2.2	MPM CAS Layout Procedure	62
4.2.2.3	Physical CAS Layout	71
4.2.2.4	Disparity Zone Layout	72
4.2.3	CAS Reset Capability	77
4.3	Design Implementation	82
4.3.1	Presence Detectors	82
4.3.2	Hardware CAS	84

TABLE OF CONTENTS (Continued)

Section		Page
4.3.3	Software CAS	90
4.3.4	Firmware CAS	96
4.3.4.1	CAS Program Design and Development Approach	99
4.3.4.2	CAS Module Design Description	101
4.3.5	Disparity Equipment	104
4.3.5.1	Disparity Detectors	104
4.3.5.2	Disparity Latch	106
4.3.6	Safe Tone Subsystem	108
5	CAS ASSESSMENT	112
5.1	Analysis	112
5.1.1	CAS Examination	113
5.1.1.1	System Logic	114
5.1.1.1.1	Main Guideway Logic	115
5.1.1.1.2	Switch Verification Logic	118
5.1.1.1.3	Priority Flip-Flop	122
5.1.1.1.4	Checked Redundant CAS Fault Tree	125
5.1.1.2	Fail-safe Circuits	126
5.1.1.2.1	Switch Verify Receiver	126
5.1.1.2.2	Loop Driver	127
5.1.1.2.3	Control Gate	129
5.1.1.2.4	Disparity Detector	131
5.1.1.2.5	Disparity Latch	133
5.1.1.2.6	Unchecked CAS Circuits Fault Tree	134
5.1.2	Problems Encountered and Their Solution	136
5.2	CAS Testing	137
5.2.1	Test Scenarios	138
5.2.2	System Integration Laboratory Tests	138
5.2.3	Logic Tests at Morgantown	140
5.2.4	Safe Tone Feedthrough Tests	143
6	POTENTIAL IMPROVEMENTS	144
6.1	Design Alternatives	144
6.1.1	Checked Redundancy Alternatives	144
6.1.2	Firmware CAS	146
6.1.3	Slide-Through Protection	147
6.1.4	Switch Verification	148
6.1.5	Merge Control	149
6.2	CAS Extensions	149
6.2.1	Short Headway	150
6.2.2	Bidirectional CAS	152
Appendix A	Glossary	A-1
Appendix B	Report of New Technology	B-1

LIST OF ILLUSTRATIONS

Figure		Page
1-1	MPM System Elements (Phase II)	2
1-2	C&CS System Design Chronology	4
2-1	Station-Vehicle Communications	8
2-2	FSK/Speed Tone Loop Control (Phase IB)	10
2-3	Calibration Loop Control (Phase IB)	11
2-4	Stop Tone Loop Control (Phase IB)	12
2-5	Switch Time Allocation Requirements Summary (Maximum Values)	13
2-6	Switch Tone Loop Control (Phase IB)	14
2-7	CAS Functional Diagram	15
2-8	Typical Vehicle Running Pads - Elevated Guideway	17
2-9	Vehicle Characteristics (Phase I)	18
2-10	Brake System Schematic	19
2-11	Vehicle Control and Communications Unit	21
2-12	VCCS Functional Block Diagram	24
2-13	CAS Control Concept	26
3-1	CAS Functional Block Diagram - Derived Requirements	35
4-1	Merge Protection	42
4-2	Slide-Through Protection	44
4-3	CAS Functional Diagram	46
4-4	Sample Layout	62
4-5	Time/Distance Plot for CAS Layout	63
4-6	Layout with Block Alignment	63
4-7	CAS Layout/Vehicle Separation vs Position	64
4-8	Definition of Safety and Operability Margins	67
4-9	Towers Station Merge Guard Loops	68
4-10	Merge Plot Example	69
4-11	PD/Safe Tone Alignment	71
4-12	Vehicles Emergency Braked vs. Number CAS Disparity Zones	74
4-13	Typical T&M Panel	78
4-14	Presence Detector Electronics	83
4-15	Hardware Block Occupancy Logic	85
4-16	Merge Protection Logic	86
4-17	Switch Verification Logic	89
4-18	Software Equipment Diagram	91
4-19	Installation of Runout Switch	95
4-20	CAS System Components	96
4-21	CAS Control Subsystem Block Diagram	97
4-22	Disparity Detector and Control Gate	104
4-23	Simplified Schematic of Disparity Latch	106
4-24	Safe Tone Subsystem	111

Figure		Page
5-1	CAS Fault Tree	113
5-2	Main Guideway Logic	115
5-3	Switch Verification Logic	118
5-4	Priority Flip-Flop Functional Diagram	122
5-5	Checked Redundancy Fault Tree	125
5-6	Loop Driver	128
5-7	Control Gate	130
5-8	Disparity Detector	131
5-9	Disparity Latch	133
5-10	Non-Checked Fault Tree	135
5-11	CAS Equipment Tested at SIL	139
6-1	Dual CAS Alternatives	145
6-2	Two-Block CAS	150

Table		Page
2-1	Signal Transmission Characteristics	9
4-1	Maximum Block Lengths	59
4-2	Maximum Number of Vehicles Emergency Braked by Disparity	75
4-3	CAS Zone Trade Data	76
4-4	Interface Signals	98

1. INTRODUCTION

1.1 GENERAL

This report summarizes the design and development work on the Collision Avoidance System (CAS) for the Morgantown People Mover (MPM) system. Since the MPM was developed in three phases, this report presents a coherent analysis of design versus experience that occurred over a 10 year span and concludes with some observations important for future usage of this type of system. This development is presented in the following sections:

Section 1. Introduction
Section 2. General System Description
Section 3. CAS Requirements
Section 4. CAS Design
Section 5. CAS Assessment
Section 6. Potential Improvements

This section and the next provide background regarding the development of the MPM system and its current configuration. The remaining sections discuss the CAS. Sections 3 and 4 discuss the conceptual and practical CAS design considerations and describe the resulting design. Section 5 outlines analysis and testing performed to verify proper CAS operation. Section 6 suggests refinements and extensions which might be considered for application to future systems.

1.2 HISTORY

The Morgantown project began in 1969 as an Urban Mass Transportation Administration (UMTA) demonstration program providing personal rapid transit between the central business district of Morgantown, West Virginia and the widely separated campuses of West Virginia University (WVU).

The MPM system (Figure 1-1) is an automated, two-mode (schedule and demand) transit system that consists of a fleet of electrically powered, rubber tired, passenger-carrying vehicles operating on a dedicated

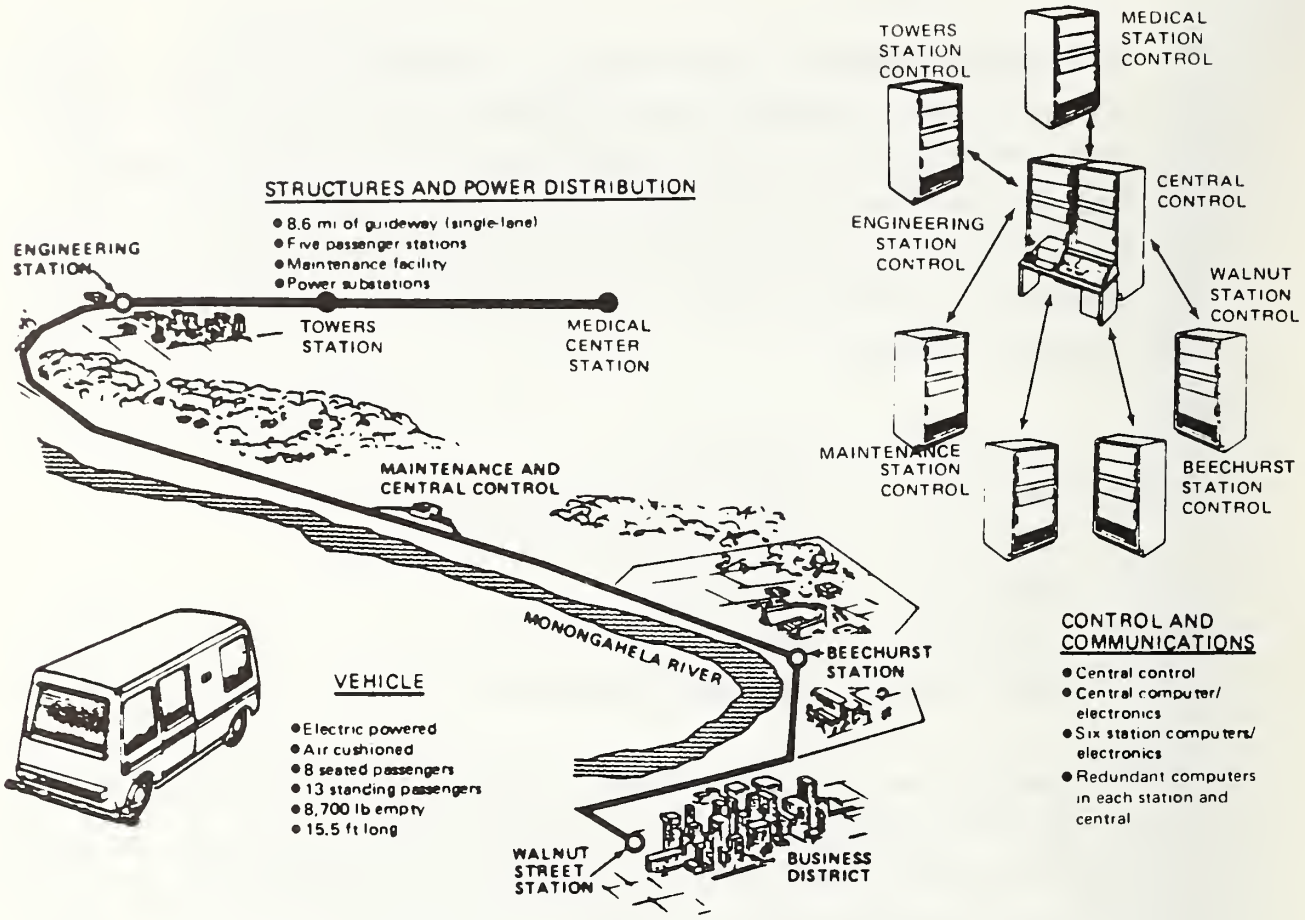


FIGURE 1-1. MPM SYSTEM ELEMENTS (PHASE II)

network guideway under computer control. The driverless vehicles automatically follow a guide rail along the guideway. The on-board switchable steering concept was originated by the Alden Company of Natick, Massachusetts. The project began with a research grant given to WVU in 1969. Initially, it was to be an expanded version of the Alden system. However, in mid-1970 it was determined that a new system would be created under requirements and constraints established jointly between WVU and UMTA. The Jet Propulsion Laboratory (JPL) of Pasadena, California was selected as system manager and designer in 1970. In May 1971 contracts were let to The Boeing Company, Seattle, Washington, for vehicle design and fabrication and to Bendix Company, Ann Arbor, Michigan, for communications and control of a six station system.

During the first half of 1971, JPL conducted a series of design trade studies resulting in the selection of a control and communications system (C&CS) incorporating the major design features of the current C&CS. The system selected included a collision avoidance system in addition to and independent of the normal operational control of vehicles. The operational control system incorporates synchronous operation of vehicles which are controlled by "point follower" as opposed to "vehicle follower" control laws. The point follower control scheme assigns vehicles to virtual time slots which conceptually move along the guideway with fixed headway according to a predetermined speed profile. The collision avoidance system independently enforces vehicle separation requirements to avoid possibility of collision should normal control malfunction.

In September 1971 with much of the system design completed, UMTA transferred system management responsibility from JPL to Boeing. Also at this time, the program was phased first to build a three-station system (Phase I) and later to expand to a six-station system in Phase II.

Phase I was divided into a Phase IA and a Phase IB. Phase IA, completed in September 1973, resulted in a prototype system comprising 5.2 miles of single-lane guideway, three passenger stations, a maintenance and central control facility, and five test vehicles. Phase IB provided the additional facilities required for public service including a fleet of 45 vehicles. Phase IB provided the opportunity to resolve problems encountered in the prototype Phase IA system. Several CAS improvements were implemented to provide fail-safe operation. Most significant was adoption of a dual redundant CAS with fail-safe disparity checking. Hard wired logic provided one leg of the dual CAS while computer software provided the second leg.

Phase IB was completed and passenger service was initiated in September 1975. Boeing was then awarded an operation and maintenance contract covering the first year of operation. During this time period many operational difficulties were resolved and desirable improvements were identified. No serious CAS problems were encountered.

The MPM system performance was adequate to encourage WVU and UMTA to decide to proceed with Phase II expansion plans. These plans provided for two new stations and 3.4 miles of additional guideway to extend service to the Towers dormatories and the WVU Medical Center. Provision was included to expand the Engineering and Maintenance stations and to improve the system reliability. In November 1976, Boeing was awarded a Phase II contract for the above expansion and 28 new vehicles. During Phase II the CAS design was essentially unchanged except for the use of microprocessors to replace hardwired logic in the new and expanded stations. This change was made to lower system costs (fabrication and maintenance) and to improve reliability.

Phase I passenger service was terminated in July of 1978 to allow guideway modification and installation of new equipment for Phase II. Installation was completed in June 1979, and passenger service was restored in July.

The above chronology is summarized in Figure 1-2.

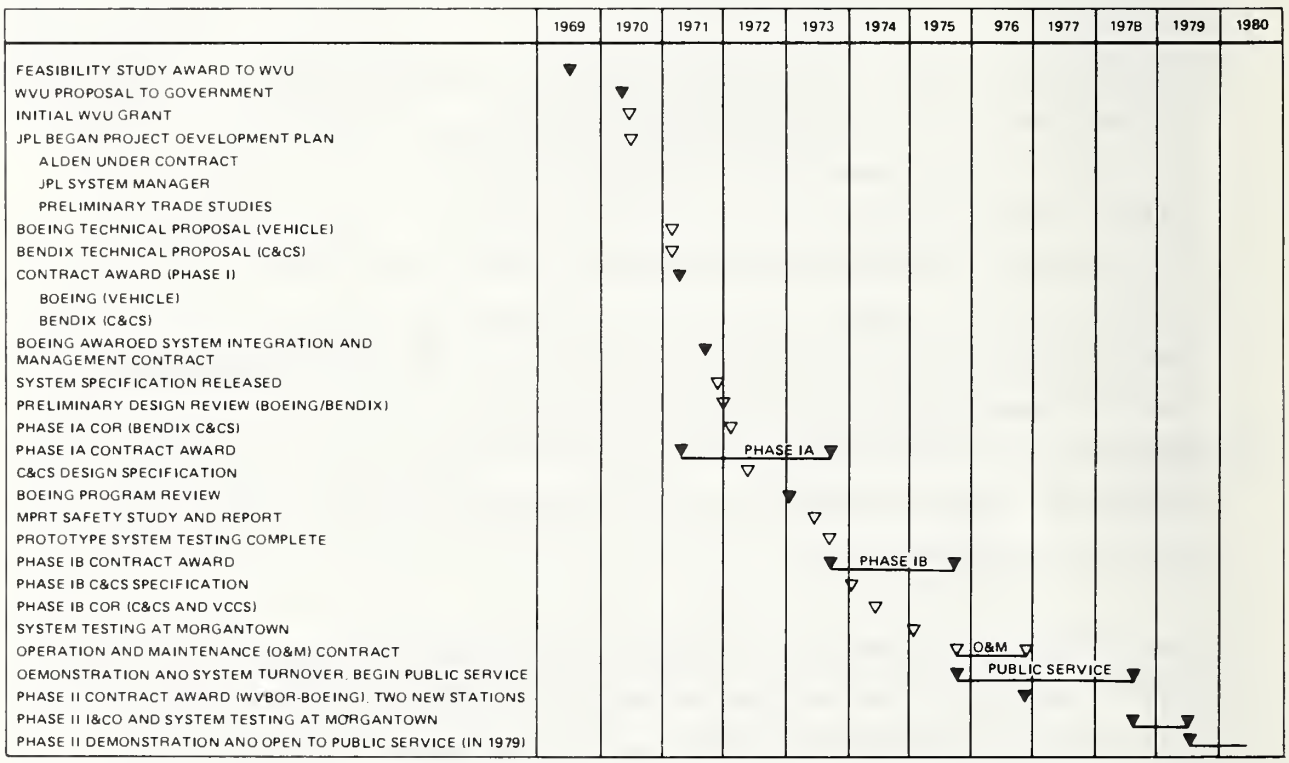


FIGURE 1-2. C&CS SYSTEM DESIGN CHRONOLOGY

2. GENERAL SYSTEM DESCRIPTION

The present operational Morgantown People Mover (MPM) system consists of the Walnut, Beechurst, Engineering, Towers, and Medical Center stations, a vehicle maintenance facility with a small test loop, a central control facility, and 73 electrically powered, rubber-tired vehicles. The five passenger stations and the maintenance station are interconnected by a dual-direction guideway network. Vehicles are dispatched and monitored by the Control and Communications System (C&CS) computers located in the central control facility and each station. Safe vehicle separation is independently ensured by the Collision Avoidance System (CAS) which monitors vehicle location by inputs from presence detectors located along the guideway. Should a vehicle approach too closely to the vehicle in front of it, the CAS will cause the vehicle to initiate emergency braking and stop. The CAS also provides protection at merges to avoid simultaneous arrivals. Vehicle speed is maintained by the onboard Vehicle Control and Communication System (VCCS) to conform to the assigned guideway civil speed that is continuously communicated to the vehicle through the C&CS. Since all vehicles respond to the same speed commands, they travel at fixed headway (time separation). This enables synchronous operation in which vehicles are assigned to travel in discrete time slots at headways which are multiples of 15 seconds.

The driverless vehicles automatically follow guiderails along the guideway. On-board switchable steering allows the vehicle to follow a guiderail on either side. Guideway junctures (merge and demerge) are negotiated by steering on the appropriate side.

The main guideway is divided into six segments, each under control of the nearest station. Under system control from the Central Control and Communications System (CCCS), the Station Control and Communication Subsystem (SCCS) performs the control and monitoring functions for local transit operations at the six stations. The station computer

commands vehicle operations (i.e., switching, stopping, and door operation). The station computer also commands the station dynamic displays and responds to inputs from the passenger-activated Destination Selection Units (DSU).

Passenger service is provided in either of two modes. In demand mode vehicle trips are assigned in response to passenger requests from the DSU. In schedule mode trips are assigned per a predefined schedule. In either case, the SCCS assigns a destination to a vehicle and commands the vehicle to open its door. After allowing sufficient time for passenger loading the door is closed. The vehicle is then assigned an unoccupied time slot on the main guideway. The vehicle is dispatched at a time synchronized to assure that main guideway entry is aligned with the assigned time slot. This is made possible by on-board "point follower" control which limits vehicle positional error to less than 1.1 second.

The vehicle accelerates to 8 ft/s and proceeds at this speed to the acceleration ramp. On the ramp, the vehicle accelerates at 2 ft/s^2 until the main guideway speed is reached. The vehicle steers right on the acceleration ramp past the merge point on the main guideway and then is commanded to steer left. Civil speed is 22, 33 or 44 ft/s on different sections of the main guideway. Speed changes are detected by the vehicle VCCS which commands speed transitions at the point follower control rate of 2 ft/s^2.

Vehicle progress on the guideway is monitored by the SCCS via vehicle presence detector (PD) inputs. The SCCS also monitors vehicle status.

Responsibility for detailed vehicle management is transferred from one SCCS to the next at a designated guideway PD. CCCS informs the receiving SCCS of the enroute vehicle identification, destination, status, and assigned point follower slot. When the vehicle arrives at the PD, the receiving SCCS takes over vehicle control and fault report monitoring tasks.

At the destination station the vehicle is commanded to steer right and exits the main guideway.

The incoming vehicle is routed to an unoccupied unloading berth by steering commands which direct the vehicle into the proper channel. Normal vehicle speed during channel switching is 8 ft/s. After the switching region is cleared, the vehicle is decelerated to 4 ft/s from which a vehicle will initiate a station stop sequence. The SCCS commands a station stop by energizing the stopping loop at the channel location where the vehicle is to unload.

In unloading positions the door is commanded open to allow passengers to depart. The door is then automatically closed and the vehicle is commanded to "move up" to the forward position in the channel (loading postion) and becomes available for another trip.

2.1 STATION CONTROL AND COMMUNICATIONS EQUIPMENT

Equipment installed on the guideway that are required to control and monitor vehicle progress include Frequency Shift Keying (FSK) and signal tone loops, switch and high-speed enable magnets, vehicle presence detectors, and the cabling required to electrically connect these elements to the station. All active electronics are located in the station C&CS equipment rooms and are powered by an uninterruptible power supply (UPS). Station-generated commands are inductively coupled to the vehicle from control loops buried in the guideway just under the running surface.

The inductive communications data link transmits vital signals by tones and nonvital signals by FSK digital data message transmissions to vehicles on the guideway. Inductive communications are accomplished using (1) guideway-embedded loop antennas, which are connected to associated transmitting and receiving units in the station equipment room, and (2) vehicle borne receiving and transmitting antennas that in turn couple signals to the vehicle borne VCCS electronics.

Loop antennas are embedded throughout the entire guideway. Each loop antenna consists of two parallel lengths of wire physically separated by 6 inches and installed in slots. Loop lengths and locations vary depending on their function. Each loop is balanced to every other loop using crossovers in appropriate loops to prevent crosscoupling of signals between two or more loops occupying the same guideway slot. All transmitting loops (uplink) are located to the right of the guideway centerline in the direction of vehicle travel. Receiving loops (downlink) are located to the left of the vehicle centerline.

Station-to-vehicle communication via the guideway loops is illustrated in Figure 2-1. The tranmissions consist of FSK data messages

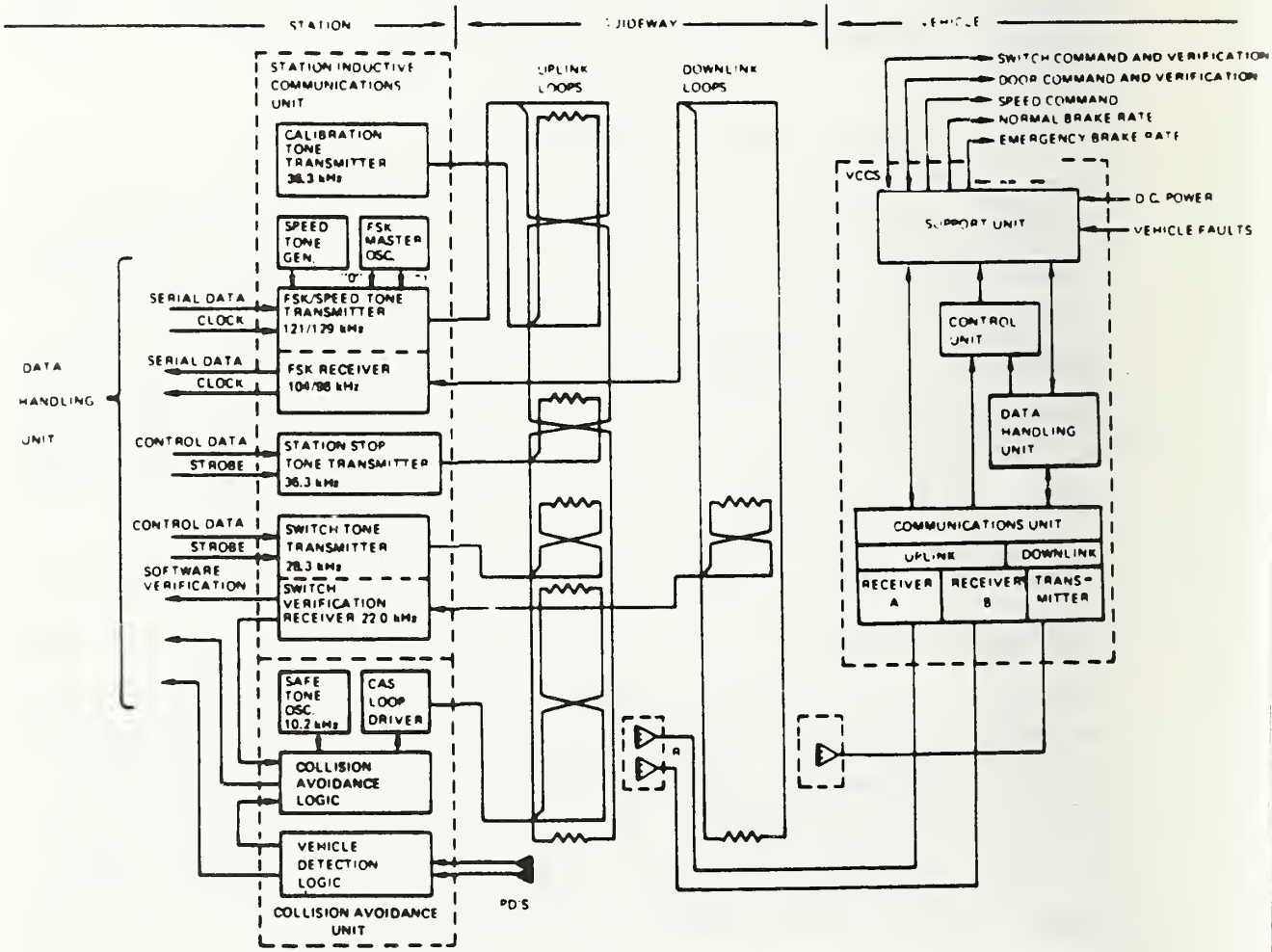


Figure 2-1. STATION-VEHICLE COMMUNICATIONS

(uplink and downlink), speed tones, switch tones, switch verification downlink tones, station stop tones, calibration tones, and safe tones (part of CAS). FSK data messages and speed tones are transmitted via common loops (uplink) that are embedded throughout the entire guideway. All other tone signals are transmitted via loops specifically dedicated to a single function though coexisting in the same guideway slots as the FSK/speed tone loops.

Vehicle-to-station communication via guideway receiving loops consists of FSK data messages and switch verification tone signals. The FSK data messages transmit vehicle status reports. FSK receiving loops (downlink) are embedded throughout the guideway opposite each FSK/speed tone transmitting loop.

Characteristics of the uplink and downlink transmissions between the vehicle and the station are shown in Table 2-1.

TABLE 2-1. SIGNAL TRANSMISSION CHARACTERISTICS

Tone type	Tone carrier frequencies (kHz)										
	6.1	10.2	13.3	17.2	22.0	28.3	36.3	96	104	121	129
Uplink											
Speed tone (44 ft/s)	50		50								
Speed tone (33 ft/s)			50	50							
Speed tone (22 ft/s)	50			50							
Speed tone (8 ft/s)	50										
Speed tone (6 ft/s)			50								
Speed tone (4 ft/s)				50							
Switch tone (right)						50					
Switch tone (left)						70					
Station stop tone							Tone only				
Calibration tone							Tone only				
Safe tone		50									
FSK										▷	▷
Downlink											
Switch verification (right)					50						
Switch verification (left)					70						
FSK								▷	▷		

Note: Numerical entries indicate modulation (ON/OFF) frequency.

Speed tones are mixed-tone signals or individual-tone signals as indicated. When two tones are present, they are phased such that they are alternately chopped at the modulation frequency.

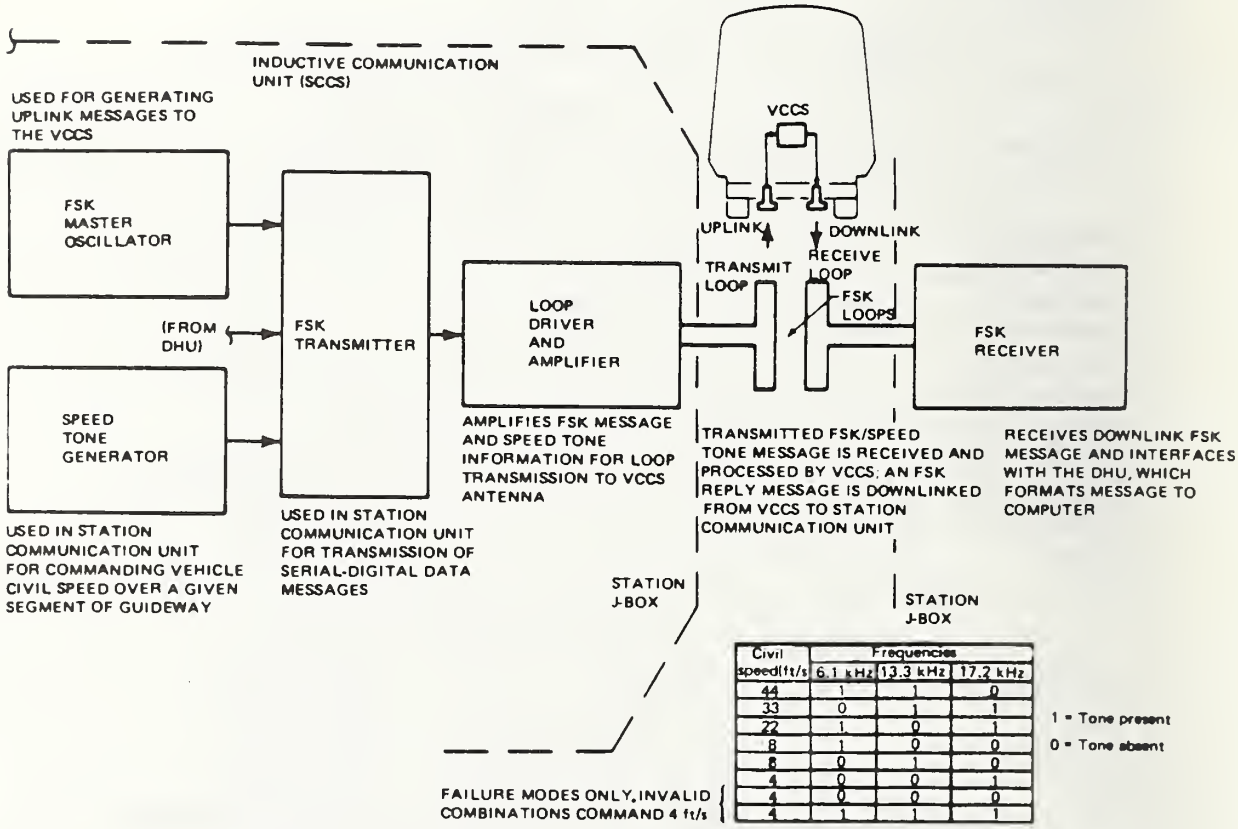
▷ FSK at 1 kHz bit rate, 50% duty cycle.

These transmissions and the corresponding control functions are described in the following paragraphs.

2.1.1 Uplink Communications

FSK and Speed Tone Control. The FSK uplink transmits speed commands and FSK messages as shown in Table 2-1.

The FSK/speed tone units consist of a master oscillator, a speed tone generator, an FSK transmitter, and a loop driver (shown in Figure 2-2). The FSK transmitter transmits computer originated vehicle commands in the form of serial data from the data handling unit. A logic "1" is represented by a 129kHz tone, and a logic "0" is represented by a 121 kHz tone.


INDUCTIVE COMMUNICATION UNIT (SCCS)
USED FOR GENERATING UPLINK MESSAGES TO THE VCCS
VCCS
FSK MASTER OSCILLATOR
(FROM DHU)
FSK TRANSMITTER
LOOP DRIVER AND AMPLIFIER
UPLINK
DOWNLINK
TRANSMIT LOOP
RECEIVE LOOP
FSK LOOPS
FSK RECEIVER
SPEED TONE GENERATOR
AMPLIFIES FSK MESSAGE AND SPEED TONE INFORMATION FOR LOOP TRANSMISSION TO VCCS ANTENNA
TRANSMITTED FSK/SPEED TONE MESSAGE IS RECEIVED AND PROCESSED BY VCCS; AN FSK REPLY MESSAGE IS DOWNLINKED FROM VCCS TO STATION COMMUNICATION UNIT
RECEIVES DOWNLINK FSK MESSAGE AND INTERFACES WITH THE DHU, WHICH FORMATS MESSAGE TO COMPUTER
USED IN STATION COMMUNICATION UNIT FOR COMMANDING VEHICLE CIVIL SPEED OVER A GIVEN SEGMENT OF GUIDEWAY
USED IN STATION COMMUNICATION UNIT FOR TRANSMISSION OF SERIAL-DIGITAL DATA MESSAGES
STATION J-BOX
STATION J-BOX
FAILURE MODES ONLY, INVALID COMBINATIONS COMMAND 4 ft/s
1 = Tone present
0 = Tone absent

Civil speed (ft/s)	Frequencies 6.1 kHz	13.3 kHz	17.2 kHz
44	1	1	0
33	0	1	1
22	1	0	1
8	1	0	0
6	0	1	0
4	0	0	1
4	0	0	0
4	1	1	1

FIGURE 2-2. FSK/SPEED TONE LOOP CONTROL (PHASE IB)

The speed-command tone signal inputs are generated in one of six possible speed tone circuit configurations that provide signal outputs corresponding to speeds of 44, 33, 22, 8, 6 and 4 ft/s.

The higher command speeds utilize circuit configurations that provide signal outputs in combinations of one or two possible tones (Table 2-1). The tones are apportioned such that a single tone defines one of the three lower speeds, and any two tones alternately chopped command one of the three higher speeds. In this manner, failure of any one oscillator in the higher speeds circuits will default to a lower speed command and, thus, remain safe.

Vehicle Calibration. The calibration tone generator transmits a signal to the VCCS to provide a distance reference. (See Figure 2-3.) This nonvital signal is used by the VCCS as a reference for calibrating the vehicle's odometer. Calibration tone loops are 200 ft long and generally positioned every 800 ft along the guideway.

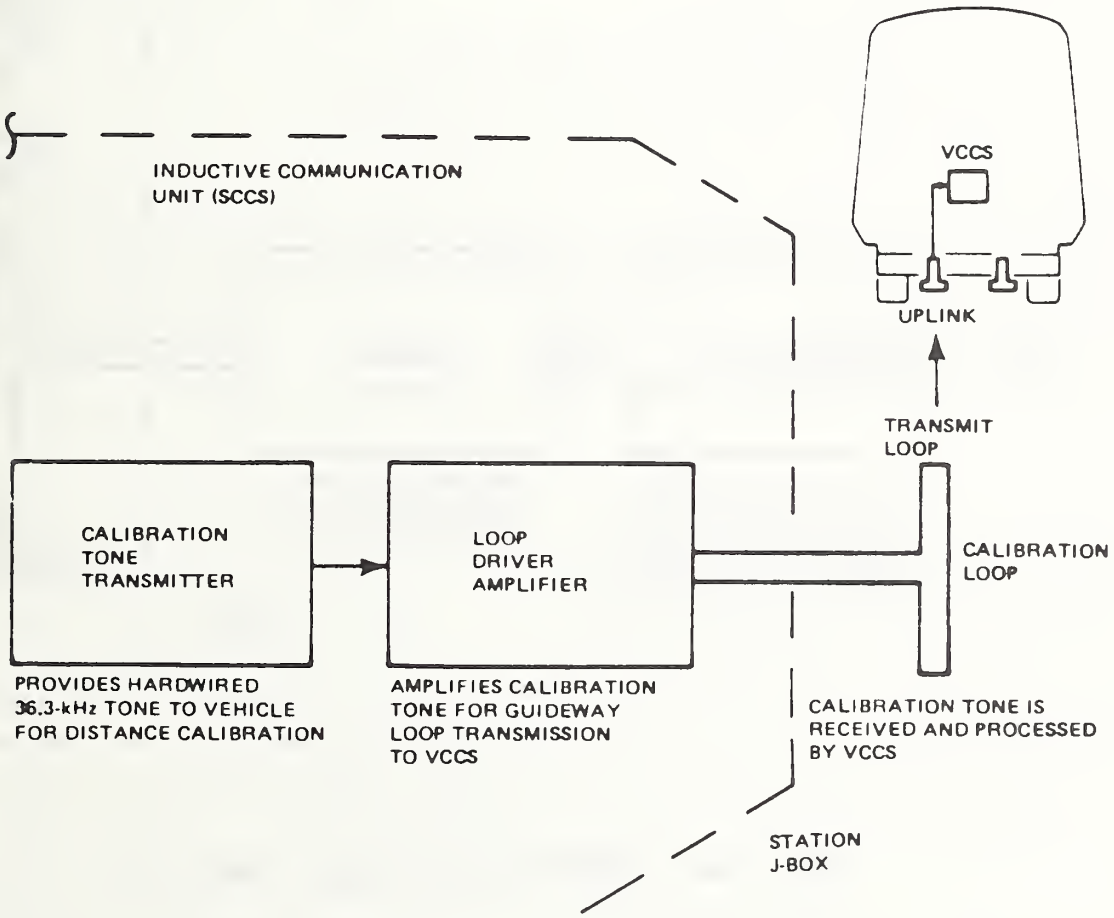

INDUCTIVE COMMUNICATION UNIT (SCCS)
VCCS
UPLINK
TRANSMIT LOOP
CALIBRATION TONE TRANSMITTER
LOOP DRIVER AMPLIFIER
CALIBRATION LOOP
PROVIDES HARDWIRED 36.3-kHz TONE TO VEHICLE FOR DISTANCE CALIBRATION
AMPLIFIES CALIBRATION TONE FOR GUIDEWAY LOOP TRANSMISSION TO VCCS
CALIBRATION TONE IS RECEIVED AND PROCESSED BY VCCS
STATION J-BOX

FIGURE 2-3. CALIBRATION LOOP CONTROL (PHASE IB)

Station Stop. When a vehicle enters a station channel, it is commanded to stop at the proper berth by the presence of a stop tone. The station stop tone units comprise a stop tone transmitter that generates a 36.3 kHz continuous tone and its associated loop driver (shown in Figure 2-4).

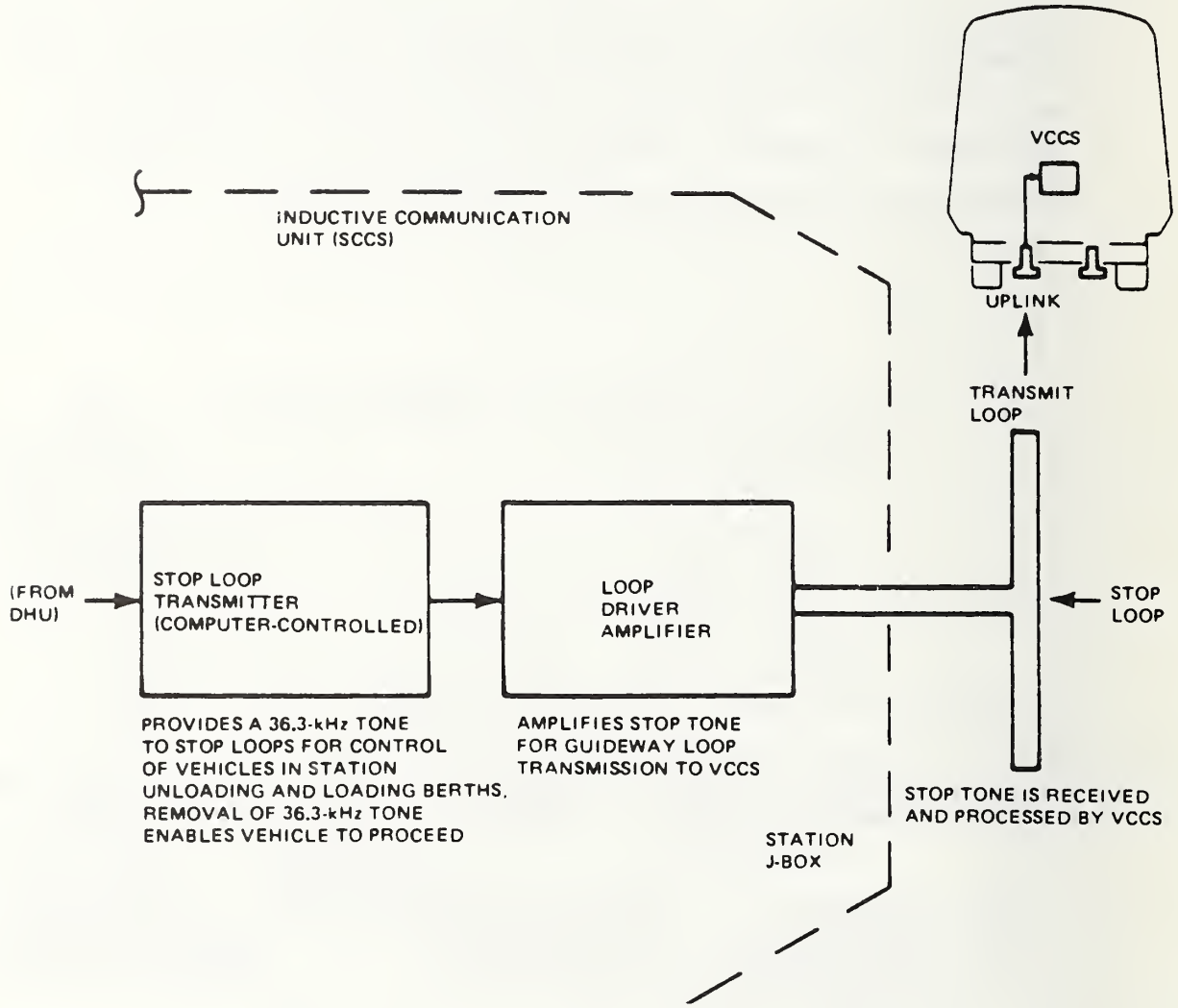

VCCS
INDUCTIVE COMMUNICATION UNIT (SCCS)
UPLINK
TRANSMIT LOOP
(FROM DHU)
STOP LOOP TRANSMITTER (COMPUTER-CONTROLLED)
LOOP DRIVER AMPLIFIER
STOP LOOP
PROVIDES A 36.3-kHz TONE TO STOP LOOPS FOR CONTROL OF VEHICLES IN STATION UNLOADING AND LOADING BERTHS. REMOVAL OF 36.3-kHz TONE ENABLES VEHICLE TO PROCEED
AMPLIFIES STOP TONE FOR GUIDEWAY LOOP TRANSMISSION TO VCCS
STOP TONE IS RECEIVED AND PROCESSED BY VCCS
STATION J-BOX

Figure 2-4. STOP TONE LOOP CONTROL (PHASE IB)

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
UMTA-MA-06-0048-80-9	PB 81-154858	

4. Title and Subtitle	5. Report Date
Morgantown People Mover Collision Avoidance System Design Summary.	September 1980
	6. Performing Organization Code: DTS-723
7. Author(s): R.J. Schroder, and R.S. Washington	8. Performing Organization Report No.: DOT-TSC-UMTA-80-37
9. Performing Organization Name and Address: Boeing Aerospace Company* Automated Transportation Systems Seattle, Washington 98124	10. Work Unit No. (TRAIS): MA-06-0048
	11. Contract or Grant No.
12. Sponsoring Agency Name and Address: U.S. Department of Transportation Urban Mass Transportation Administration 400 Seventh Street, S.W. Washington, D. C. 20590	13. Type of Report and Period Covered: Final Report
	14. Sponsoring Agency Code: UTD-60

15. Supplementary Notes

*Under contract to: U.S. Department of Transportation, Research & Special Programs Administration, Transportation Systems Center, Kendall Square, Cambridge, MA 02142

16. Abstract

The Morgantown project began in 1969 as an UMTA demonstration program providing personal rapid transit between the central business district of Morgantown, West Virginia, and the widely separated campuses of West Virginia University. The Morgantown People Mover (MPM) is an automated two-mode (schedule and demand) transit system that consists of a fleet of electrically powered, rubber-tired, passenger-carrying vehicles operating on a dedicated guideway under computer control. The present operational MPM system consists of 5 stations, a vehicle maintenance facility with a small test loop, a central control facility, and 73 electrically powered, rubber-tired vehicles.

This report describes the Collision Avoidance System (CAS) design used for the current (1980 Phase II) MPM system. It presents historical data leading to the current design. The report also includes results of experience with the CAS, plans for system improvements, and recommendations for future designers of such systems. Identification of safety and operability requirements led to a unique implementation of a proven safety concept--block occupancy control. Problems encountered and the design solutions which evolved are discussed with emphasis upon fail-safe features. The resulting CAS design is assessed and found to be extremely safe. Possible improvements and extensions are discussed. Shorter headway and bi-directional operations are found to be feasible. This report contains a glossary of terms and many charts illustrating the elements of the MPM system.

17. Key Words	18. Distribution Statement
Automated Guideway Transit Morgantown People Mover Collision Avoidance Headway Block Occupancy Fail-Safe AGT Safety University Transit	Available to the Public through the National Technical Information Service, Springfield, Virginia 22161.

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
Unclassified	Unclassified	168	A08

Form DOT F 1700.7 (8-72) Reproduction of completed page authorized

The station stop tone transmitter is controlled by a computer-generated command data word that is decoded by the Data Handling Unit (DHU) to control the addressed station stop tone unit. The VCCS must be receiving a 4 ft/s speed command and a stop tone for 4.5 inches of travel to begin the deceleration profile that will allow the vehicle to stop at the berth. After the vehicle has come to rest, it may be dispatched again by removing the stop tone. When the vehicle is dispatched, it will follow an acceleration profile of 2 ft/s^2 up to the assigned civil speed.

Switch Tone Control. The switch tone transmitter generates a signal to command a vehicle to "steer left" or "steer right." The vehicle is sent a switch command as it passes over the switch loop at every guideway juncture (merge or demerge). The vehicle, regardless of its previous switch position, must verify that it is in the position dictated by the switch loop command or it is brought to a stop via an interlock to the CAS. When a switch command is received , the action and verification must take place within the time allocation shown in Figure 2-5.

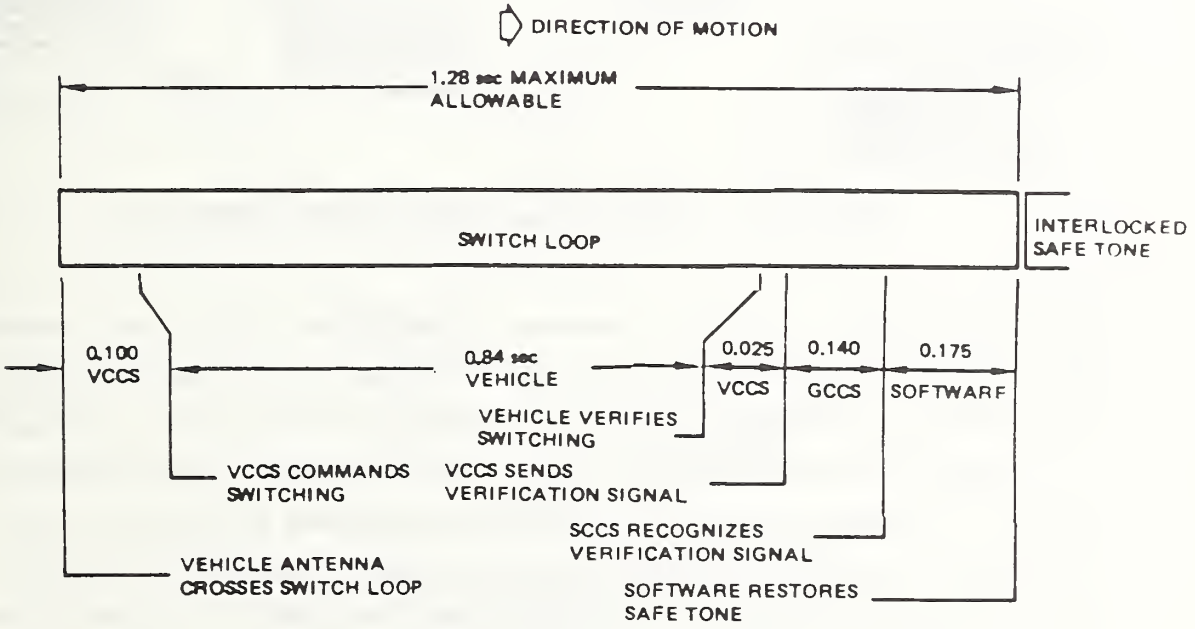


FIGURE 2-5. SWITCH TIME ALLOCATION REQUIREMENTS SUMMARY (MAXIMUM VALUES)

Switch tone units used to control vehicles entering guideway demerge zones consist of a computer-controlled transmitter, a loop driver, and the associated loop. Switch tone units used to control vehicles entering guideway merge zones employ a fixed "steer right" or "steer left" switch tone transmitter, a loop driver, and the associated switch loop. Figure 2-6 shows the functional block diagram of the switch tone control units.

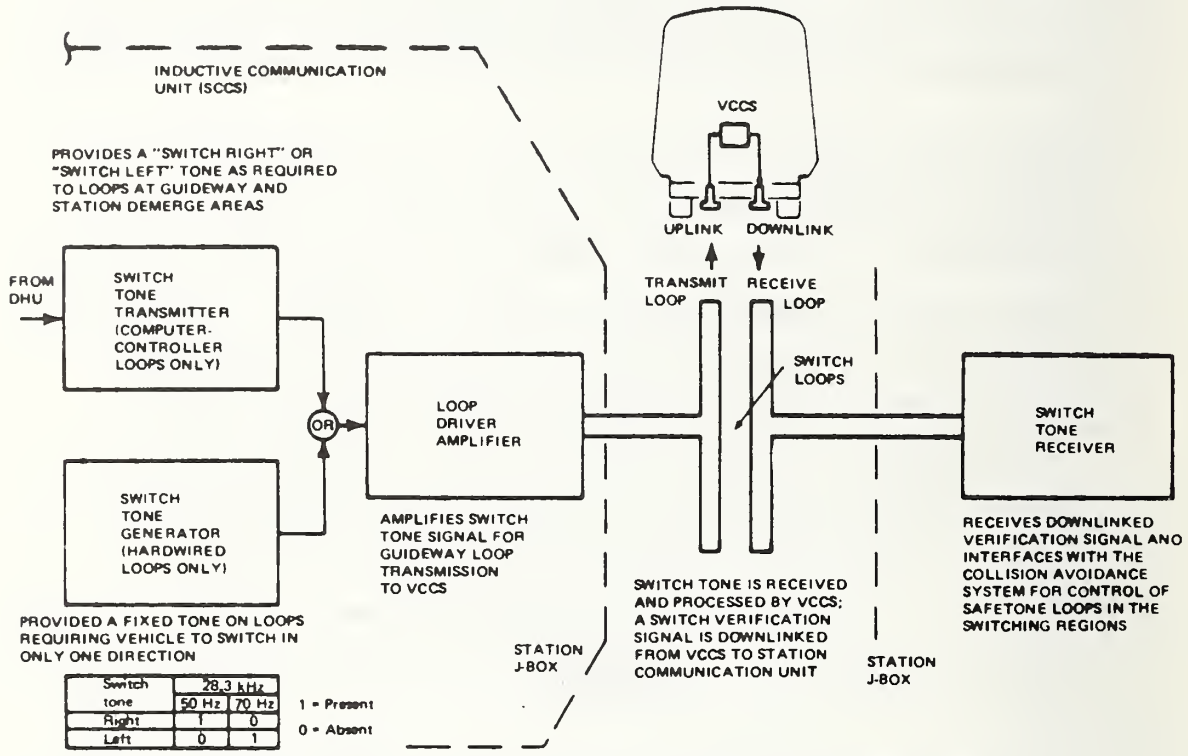

INDUCTIVE COMMUNICATION UNIT (SCCS)
PROVIDES A "SWITCH RIGHT" OR "SWITCH LEFT" TONE AS REQUIRED TO LOOPS AT GUIDEWAY AND STATION DEMERGE AREAS
VCCS
UPLINK
DOWNLINK
TRANSMIT LOOP
RECEIVE LOOP
FROM DHU
SWITCH TONE TRANSMITTER (COMPUTER-CONTROLLER LOOPS ONLY)
OR
LOOP DRIVER AMPLIFIER
SWITCH LOOPS
SWITCH TONE RECEIVER
SWITCH TONE GENERATOR (HARDWIRED LOOPS ONLY)
AMPLIFIES SWITCH TONE SIGNAL FOR GUIDEWAY LOOP TRANSMISSION TO VCCS
RECEIVES DOWNLINKED VERIFICATION SIGNAL AND INTERFACES WITH THE COLLISION AVOIDANCE SYSTEM FOR CONTROL OF SAFETONE LOOPS IN THE SWITCHING REGIONS
PROVIDED A FIXED TONE ON LOOPS REQUIRING VEHICLE TO SWITCH IN ONLY ONE DIRECTION
SWITCH TONE IS RECEIVED AND PROCESSED BY VCCS; A SWITCH VERIFICATION SIGNAL IS DOWNLINKED FROM VCCS TO STATION COMMUNICATION UNIT
STATION J-BOX
STATION J-BOX
Switch tone | 28.3 kHz | 50 Hz | 70 Hz
Right | 1 | 0
Left | 0 | 1
1 = Present
0 = Absent

FIGURE 2-6. SWITCH TONE LOOP CONTROL (PHASE IB)

Safe Tone Control. Vehicle movement is permitted only in the presence of a safe-to-proceed signal called a safe tone. Safe tone absence automatically initiates irrevocable emergency rate braking. The guideway is segmented into CAS control blocks containing safe tone transmission loops. Safe tone control is provided by redundant CAS logic. One logic path interfaces with the station computer (software), and the other logic path consists of hardware CAS circuitry. A disparity detector compares signals from each of the dual CAS logic paths and removes the safe tone on the loops if the logic paths disagree.

The safe tone signal is generated for an entire station by a safe tone master oscillator generating a carrier frequency of 10.2 kHz. Unlike the other control tones, a modulation is not applied at this point. The 50Hz chopping frequency is generated at a master oscillator located in the central control facility and fed to a slave oscillator card in each station. The 50Hz frequency then is routed in a series manner (Figure 2-7) through the various disparity detectors and the zone disparity

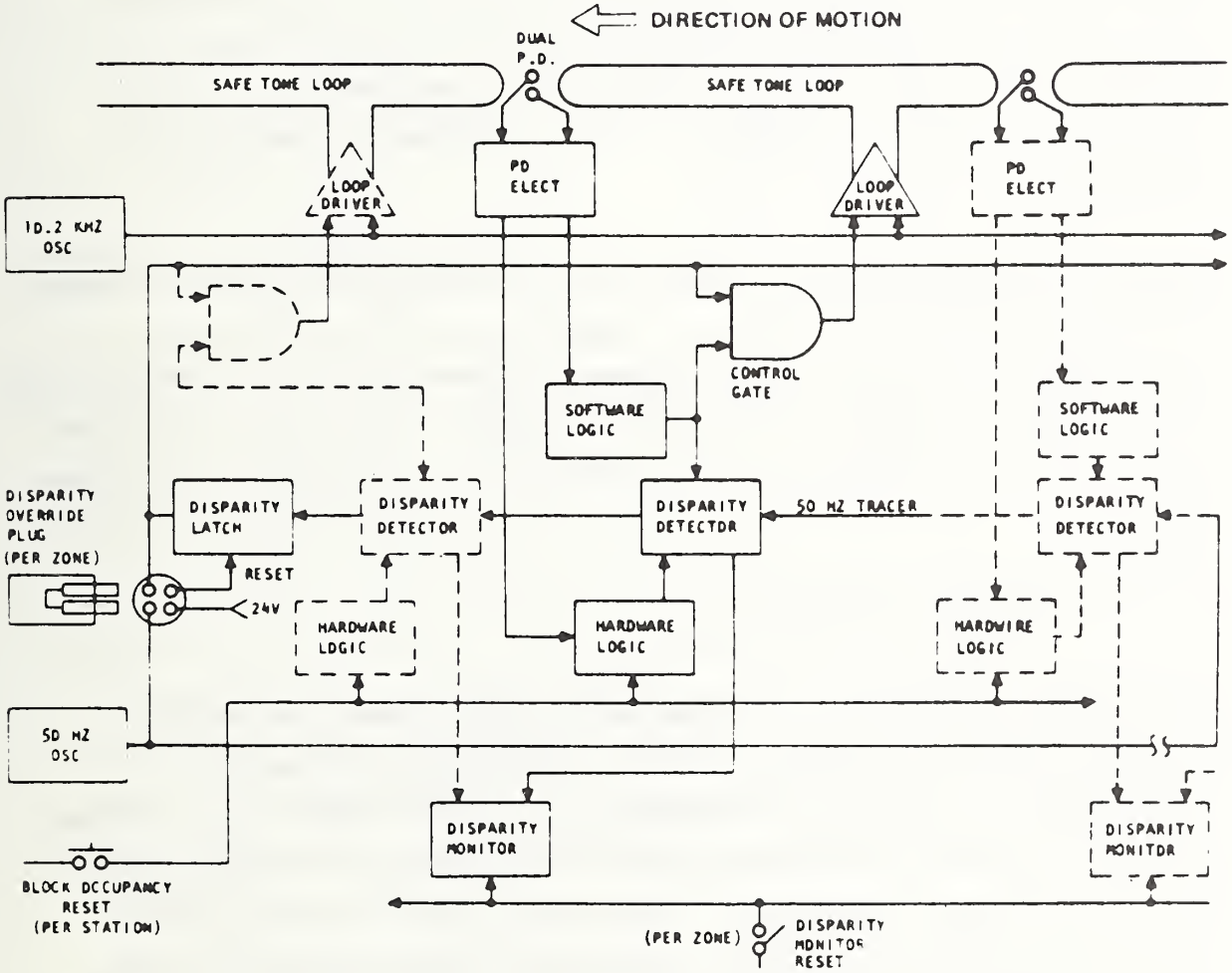


FIGURE 2-7. CAS FUNCTIONAL DIAGRAM

latch. It then is routed to a special safe tone loop driver that both applies the chopping and provides the drive current resulting in a 10.2kHz, 50Hz chopped, unbalanced safe tone signal being fed to the appropriate loop. Thus, when a control gate is turned on, the 50Hz chopping is applied to the safe tone carrier, and when the gate is turned off, the chopping is removed.

2.1.2 Downlink Communications

Vehicle FSK Downlink. The vehicle downlinks an FSK message in the same format as the station uplink using 104 kHz for a "1" and 96 kHz for a "0". The vehicle FSK downlink is received by the FSK receive loop and routed to the station receiver which converts the signal to a serial bit stream. This data is sent to the station computer via the DHU.

Switch Verification. When a vehicle has successfully switched in response to a command from a switch loop, it downlinks a switch verification signal which is a 22 kHz signal chopped at either 50 or 70 Hz corresponding to the chopping frequency of the uplink command. The signal is received by the switch verification loop and processed in the station verification receiver.

2.2 GUIDEWAY SUBSYSTEM

The guideway structure is a limited-access route connecting the MPM stations and the maintenance facility. Approximately 60 percent of the guideway is elevated; the remainder is at ground level. The running surface is concrete and contains distributed piping for guideway heating to allow all-weather operation. Steering and electrical power rails are mounted beside the guideway. Emergency walkways, handrails, and guideway lighting are provided for passenger safety if egress is required. Figure 2-8 shows a cross section of an elevated portion of the guideway. Positioning the steering rail near the running pads becomes the critical factor in vehicle antenna tracking.

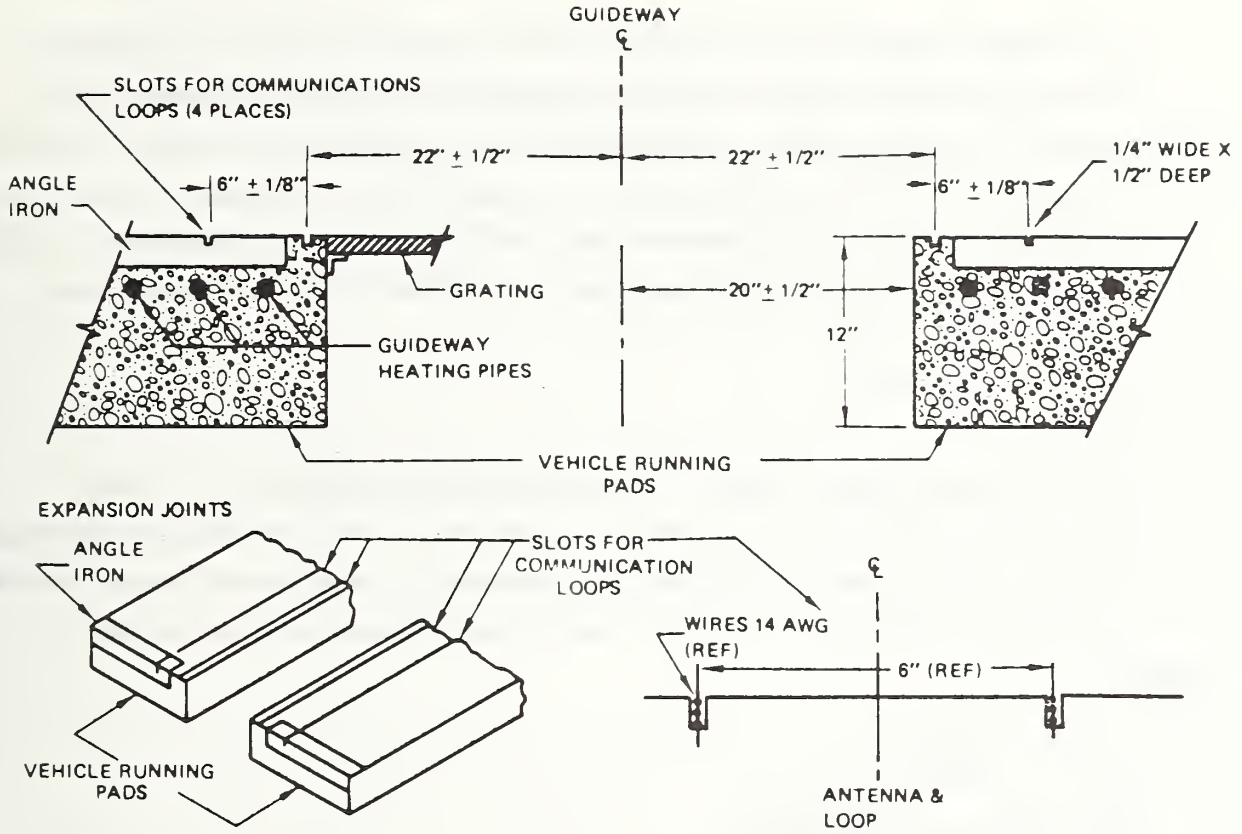


FIGURE 2-8. TYPICAL VEHICLE RUNNING PADS - ELEVATED GUIDEWAY

Inductive communications loops are installed in slots on either side of the guideway, just inside the running pads. The slots are located such that their centerline will correspond to the antenna tracking centerline of the vehicle. Two parallel slots 6 inches apart are required for each set of loops (uplink and downlink). Slot depth is selected such that the maximum number of loops required will fit without protruding above the guideway surface. Once loops are installed, the slots are filled with an epoxy compound to provide physical and environmental protection.

Uplink loops are located on the right side of the guideway (as viewed in the direction of motion), and downlink loops are on the left side. In the uplink slots, there are a minimum of two loops (safe tone and FSK) in all areas of the guideway. In station berthing areas, a third loop is added for stopping. At merges and demerges, a third loop is added for switch information. Calibration loops form a third loop

at certain intervals, and there is the possibility that a calibration loop could occur near a merge or demerge thus placing a switch tone loop in the slot also. Consequently, a maximum of four loops is possible in an uplink slot. The downlink is simpler with a maximum of two loops. There is always an FSK receive loop, but at merges and demerges a switch verification loop is added opposite the uplink switch command loop.

2.3 VEHICLES

The MPM system uses rubber-tired vehicles characterized in Figure 2-9. Each vehicle has ten major subsystems: passenger module, environmental control unit, chassis, hydraulics, pneumatics, electrical power, propulsion, steering, braking, and vehicle control and communications system.

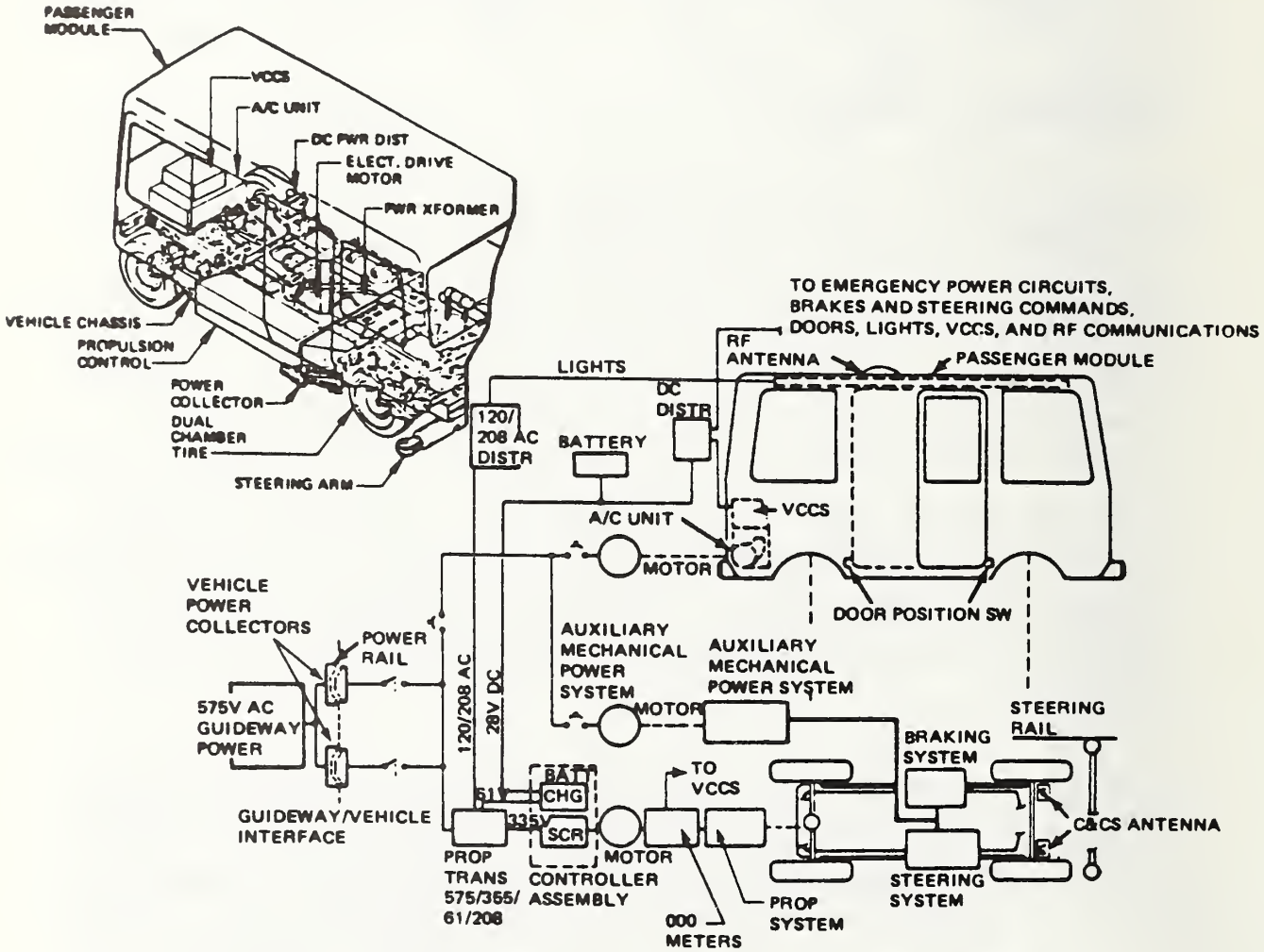


FIGURE 2-9. VEHICLE CHARACTERISTICS (PHASE I)

Commands are transmitted to the vehicle from the communication loops through antennas located on the underside of the vehicle and routed to the Vehicle Control and Communications System (VCCS). The commands control the vehicle motor, brakes, steering, and doors. Three-phase, 575 volt power is supplied to the vehicle through power rails, which can be located on either side of the vehicle, and is picked up via a power collector arm. Guide wheels located on both sides of the vehicle extend and contact a steering rail which then is followed until the vehicle is commanded by a switch tone to steer on the other side for a merge or demerge. The guide wheel controls a hydraulic, four-wheel power steering subsystem. The pneumatic system provides an automatic vehicle-leveling control. The redundant four-wheel disc brakes are hydraulically operated in response to input commands from the VCCS.

The vehicle brake system, which generates the braking torque required to decelerate or stop the vehicle, is a dual system, either one of which can stop the vehicle safely. The major components consist of two brake amplifiers, two servo valves, and four brake calipers (one per wheel). The system is redundant and independent up to the brake pads. The brakes are discs on all four wheels with a single caliper and rotor at each wheel. A schematic of the complete brake system is given in Figure 2-10.

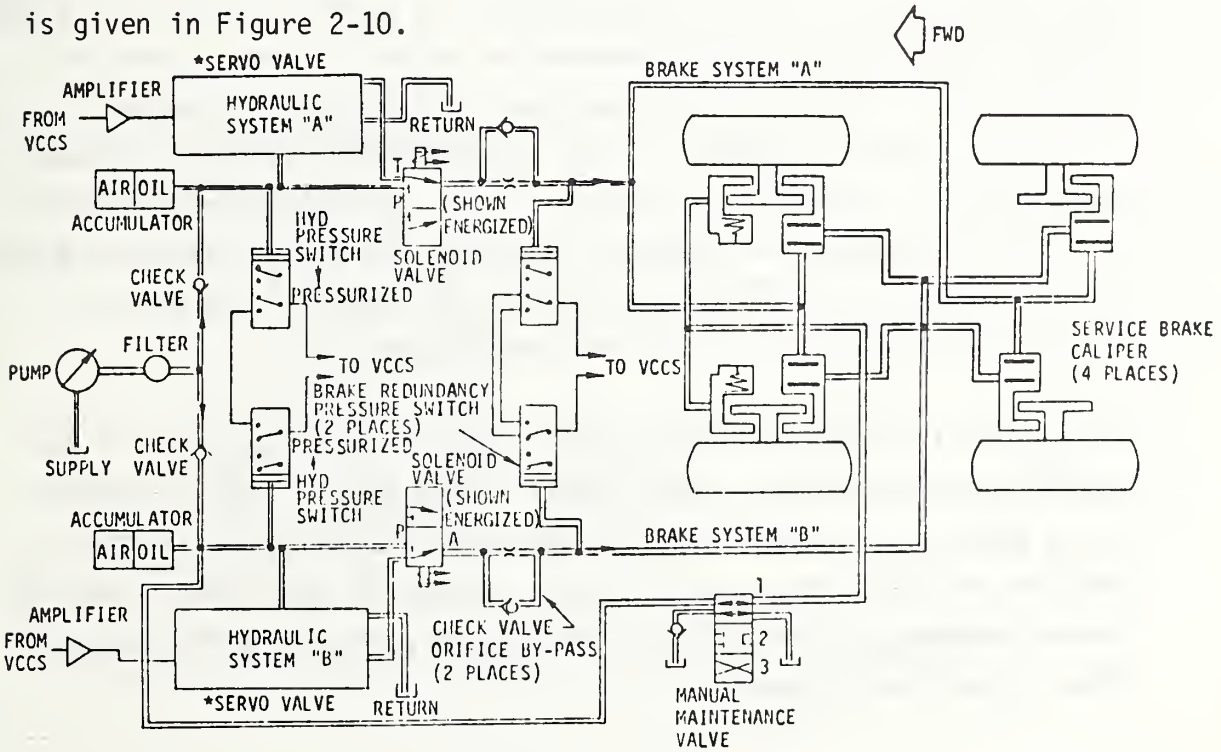


FIGURE 2-10. BRAKE SYSTEM SCHEMATIC

Redundant braking signals come from the VCCS to the brake amplifiers. The brake amplifiers command the servo valves (hydraulic pressure regulators) to respond, and the servo valves apply the proper pressure (20 to 900 psig) to the calipers. There are two braking modes: normal and emergency. The nominal normal mode deceleration is 2 ft/s^2 (0.0625 g) with the brake system providing a brake force capability in excess of 0.2 g to compensate for grades and controller lags. The emergency mode releases up to 900 psig to the calipers which results in a nominal emergency rate deceleration of 0.3 g. For Phase I, emergency braking was open loop using constant force. The current (Phase II) system uses variable braking force to provide controlled rate (closed loop) deceleration. This change has reduced the worst case stopping distance.

The brake calipers contain tandem piston actuators with independent hydraulic actuation. Either piston in the caliper assembly is able to actuate the brakes at full capacity; but when both pistons are actuated, which is normal, the braking results are not additive. Functionally, the tandem pistons perform the voting function for the redundant system with braking torque being proportional to the highest (safest) of the two input pressures.

Brake energy and control are provided by the hydraulic and the electrical systems respectively. In the absence of either or both, hydraulic energy is provided from the accumulators and energy for control is provided from the batteries. In an extreme case, when loss of power and failure of the batteries might occur, a special emergency braking system is activated; two solenoid valves in the system open upon absence of DC voltage, by-pass the servo valves, and dump all the energy in the accumulators directly into the brake calipers.

Two hydraulic pressure switches continuously monitor pressure in the accumulators and issue a fault signal to the VCCS if either pressure falls below a specified level. A second pair of pressure switches monitor the servo valve output control pressures and report a loss of brake redundancy to the VCCS if the control pressures differ by more than a specified tolerance.

Independent parking brake calipers are mounted on the front wheels and are spring loaded assemblies which are held off by hydraulic pressure. In the event hydraulic pressure decays to an unsafe level, the parking brakes automatically come on and provide a fail-safe backup to the primary system.

2.4 VEHICLE CONTROL AND COMMUNICATIONS SUBSYSTEM (VCCS)

The VCCS is located in the rear of the vehicle above the environmental control unit (ECU). The VCCS is that portion of the C&CS that is carried on board the vehicle (shown in Figure 2-11).

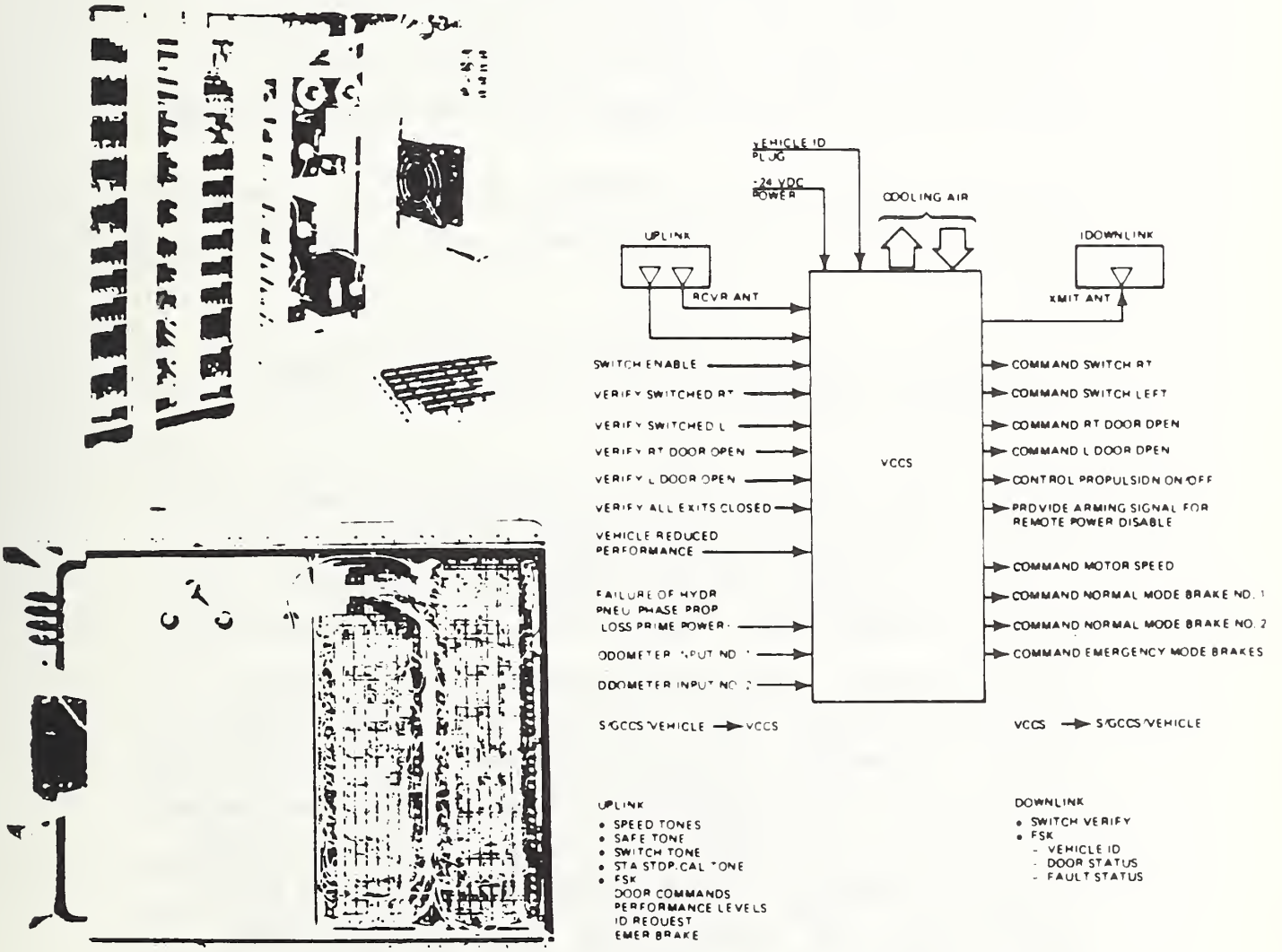


FIGURE 2-11. VEHICLE CONTROL AND COMMUNICATIONS UNIT

The VCCS receives uplink commands, provides control commands to the vehicle, and identifies and transmits downlink vehicle status to the SCCS. The VCCS responds to guideway inductive communications and vehicle inputs to regulate vehicle speed and control vehicle doors, brakes, and switching functions.

The VCCS also provides commands to the vehicle to ensure safe operation. An overspeed detector commands emergency rate braking if the vehicle exceeds a safe tolerance on commanded guideway speed. The VCCS also applies emergency brakes when it senses loss of safe tone from the inductive communications system. The VCCS monitors vehicle status, and if an unsafe condition is detected, it stops the vehicle and transmits a message via the FSK link to the station thence to the central system operator.

The VCCS is composed of the following functional units: antennas, communications unit, data handling unit, control unit, and support unit.

This report is concerned only with VCCS functions relevant to CAS design and operation.

Antennas. Two antenna assemblies provide two-way communications with the SCCS through the buried loops. One antenna assembly is used for receiving, the other antenna for transmitting. The antennas are mechanically fixed to the vehicle and electrically linked to the VCCS. The receiving antenna assembly actually contains two antennas (part of the vehicle's redundant uplink system). The antennas are vertically mounted loops in a "bifilar" configuration to reduce interference from external noise sources, such as vehicle power surges. The transmit antenna is a single horizontal rectangular fixture with multiple turns of a small conductor wire. The receive antenna is located on the right side of the vehicle and the transmit on the left. Both are located in the forward portion of the vehicle about even with the front axle and are suspended 1-1/8 in. above the guideway.

Communications Unit. The communications unit of the VCCS consists of a downlink transmitter and dual redundant uplink receiver circuitry to provide signals to and to receive signals from the guideway. Uplink communications consist of FSK messages, safe tone, switch tone, and calibration tones. Downlink communication is an FSK status message and switch verification tones verifying the response of the vehicle to a switching command. A VCCS functional block diagram is shown in Figure 2-12. Only safe tone and switch communication are relevant to the CAS.

A safe tone with a tone frequency of 10.2 kHz, chopped at a 50 Hz rate is transmitted to the vehicle. The safe tone receivers are capable of detecting the safe tone and the 50 Hz modulation and producing a logic output in less than 70 ms. Upon loss of the safe tone or its modulation, the receiver will reset the logic level in less than 115 ms. The VCCS then commands emergency rate braking.

Steering tones are transmitted to the vehicle with a 28.3 kHz frequency. The "steer right" command will chop the 28.3 kHz at a 50 Hz rate, and the "steer left" command will chop the 28.3 kHz at a 70 Hz rate. The steering tone receiver detects these signals and produces logic level outputs to indicate that a "switch right" or a "switch left" command has been detected. Steering verification signals are transmitted with a 22 kHz carrier frequency chopped by the 50 or 70 Hz previously derived from the switch command. A single vehicle antenna transmits switch verification and FSK downlink messages to the guideway receive loops.

Longitudinal Control. The Control and Communications System (C&CS) automatically controls the position of each vehicle by means of a synchronous point follower system. The point follower system consists of a series of conceptual moving points or slots referenced to a fixed time base. These theoretical points, as viewed from a fixed position on the guideway, pass at intervals which are multiples of 15 seconds. Vehicles are assigned to theoretical points by control of their dispatch times.

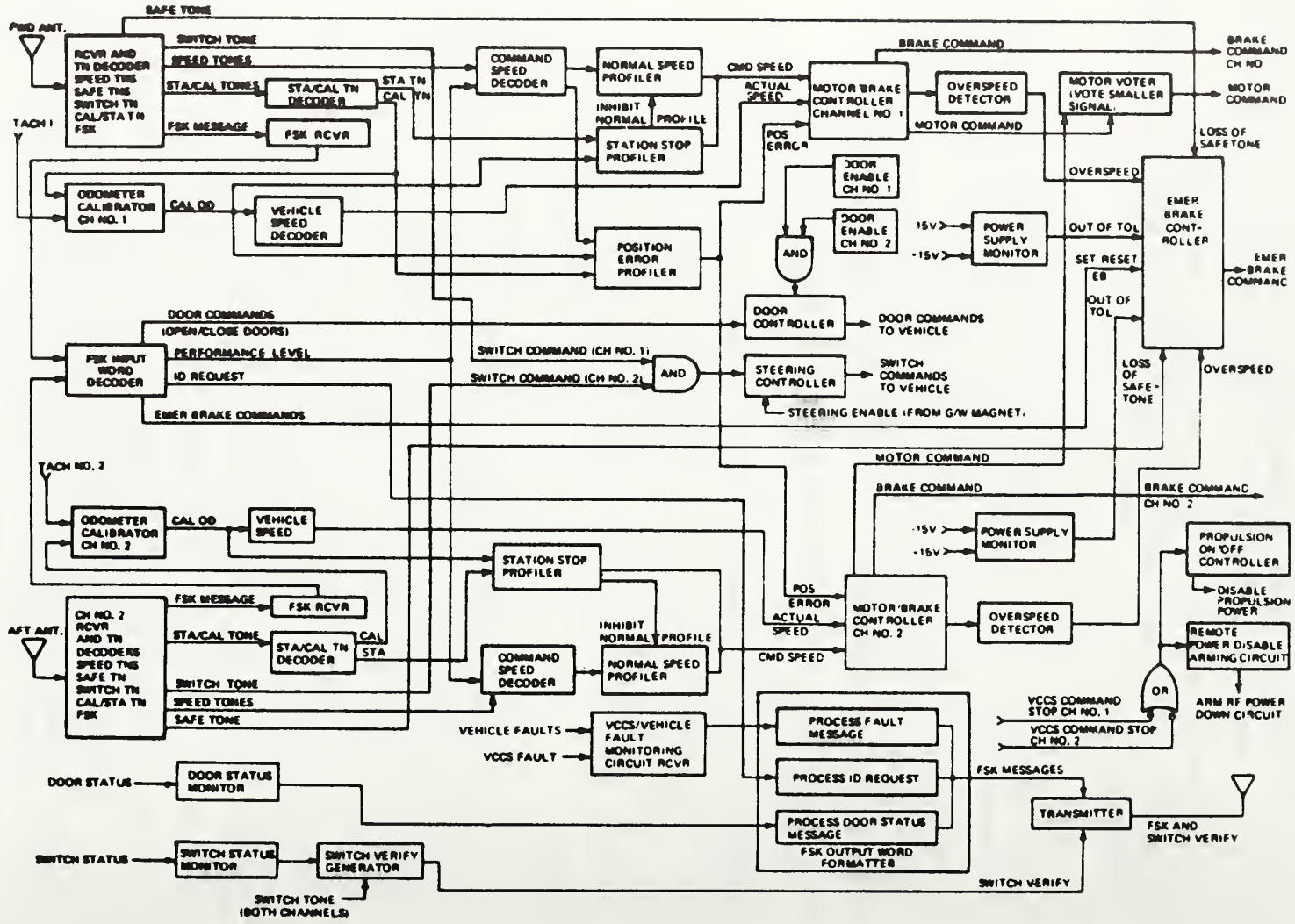


Figure 2-12. VCCS FUNCTIONAL BLOCK DIAGRAM

Once dispatched, the vehicle control unit generates an on-board point which closely approximates the assigned point maintained by the C&CS computers. The VCCS issues the brake and motor commands required to follow the on-board point.

The theoretical point position is defined as the integral of the acceleration limited civil speed command. The vehicles receive discrete civil speed commands (4, 8, 22, 33 or 44 ft/s) from the guideway with changes in speed command occurring at fixed guideway locations. The theoretical point speed is equal to the civil speed command except that changes in speed are made at an acceleration/deceleration rate of 2 ft/s^2.

The major longitudinal control function of the VCCS is to generate the brake and motor commands required to produce the specified speed-position time vehicle trajectory. This is accomplished by first computing an acceleration-limited speed command and by measuring speed and position error signals using digital circuitry to achieve the required accuracy. Two separate channels driven by redundant antennas and tachometers are used to maximize safety. The redundant motor commands are compared and the lowest (safest) is sent to the propulsion system. Both redundant brake commands are sent to the brake system where the brake calipers ultimately vote the highest (safest) command.

2.5 COLLISION AVOIDANCE SYSTEM

The Collision Avoidance System (CAS) provides protection against the possibility of vehicle collisions. The CAS protects vehicles against three types of collision:

1. Collision between adjacent vehicles traveling in the same direction,

2. Collision between conflicting vehicles traveling on merging paths, and

3. Collision between a vehicle and the guideway due to a switching failure.

Protection is not required against collision caused by opposing vehicle movement since each guideway segment is dedicated to traffic flow in a single direction and will not support movement in the reverse direction.

The CAS protection incorporates the fail-safe principle: vehicle movement is permitted only in the presence of an active safe-to-proceed signal (safe tone) controlled by checked redundant logic. Any failure which produces an erroneous safe tone signal causes vehicles to stop.

The CAS logic is based upon check-in/check-out block occupancy control. The guideway is segmented into CAS control blocks containing safe tone transmission loops. The CAS will not allow a second vehicle to enter an occupied block. As shown in Figure 2-13, vehicle separation is enforced by inhibiting the safe tone behind each occupied block. Each block length exceeds the worst case stopping distance for trailing vehicles. Thus, adjacent vehicles cannot collide even if the lead vehicle stops instantly.

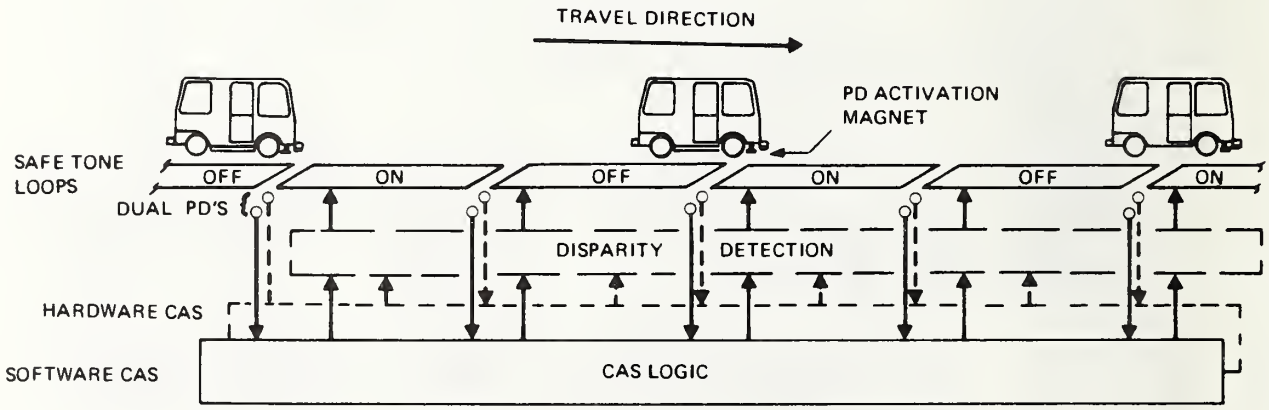


FIGURE 2-13. CAS CONTROL CONCEPT

Block occupancy information is provided by presence detectors activated by a magnet mounted on each vehicle. A block is set occupied by activation of the presence detector (PD) at the block entry. The block is cleared by activation of the departure PD. The departure PD for one block is the entry PD for the next block. Thus, a block cannot be cleared without setting the next block occupied.

Block occupancy is monitored by utilizing dual redundant PDs. One set of PDs interfaces with software CAS logic contained in a general purpose computer. The other set drives hardware CAS logic. (The original hardware CAS consisted of special built hardwired logic. Programmable microprocessor logic has replaced the hardwired logic in the new Phase II stations.) Safe tone control is provided by the software. The safe tone status specified by software CAS is compared to that specified by the hardware CAS. Any disparity removes all safe tones in the vicinity.

The collision avoidance requirements and the resulting CAS design are discussed more fully in the next two sections.

3. CAS REQUIREMENTS

The purpose of the CAS is to prevent collisions between vehicles if safe minimum vehicle headway is violated for any reason. Ideally it should perform in such a manner that the possibility of a collision, even at low vehicle speed, is eliminated in those areas of the guideway protected by CAS. The CAS must perform this function without adversely impacting system operation and must be implemented in such a manner as to facilitate maintenance. These considerations are addressed in the following paragraphs.

3.1 Safety

Since the purpose of CAS is safety, it must perform this function with a high degree of confidence. The following paragraphs explain safety in the context of the Morgantown system and the CAS safety requirements.

3.1.1 Definitions

Safety: Freedom from those conditions that can cause death or injury to personnel, damage to or loss of equipment or property.

System Safety: The optimum degree of safety within the constraints of operational effectiveness, time and cost, attained through specific application of management and engineering principles throughout all phases of the system's cycle.

Fail-Safe: No plausible failure or group of failures shall cause an unsafe condition (see also paragraph 3.1.2.1).

Fault: A component state of existence (does not have to be a failure) that contributes to a possible mode of of occurrence of an undesired event.

Incident: A minor episode or occurrence in which there is no injury to personnel but in which an unscheduled work stoppage or the removal and replacement of end item components may result.

Accident: An unplanned event which results in injury to personnel and/or property damage during any operation or activity.

Hazard: Any existing or potential condition that can cause death or injury to personnel, or damage to or loss of equipment or property.

MPM Safety Specifications (As defined in WVBOR-TD-001):

The total probability of accidental fatality of passengers on PRT vehicles shall be no greater than $1 \times 10^{-4} \times \frac{MII}{MI}$ per operational day; where:

MII = the total vehicle miles logged during the first year of revenue service for the five station PRT system (estimated 1,500,000).

MI = the total vehicle miles logged during the first year of revenue service of the three station PRT system (615,000).

The total probability of serious injuries of passengers on PRT vehicles shall be no greater than 6×10^{-3} per operational day.

The total probability of accidental major damage to system or public equipment or property shall be no greater than $2.8 \times 10^{-4} \times \frac{MII}{MI}$ per operational day (major damage is defined as that which incurs repair costs greater than $20,000).

3.1.2 Safety Requirements

Safety requirements for the CAS can be conveniently split into two categories: First, the basic safety requirements based upon the function CAS is to perform, and which are expressed at the conceptual level; Second, the derived requirements consisting of more specific criteria, which it has been determined must be designed into the system in order to meet the basic requirements. These two categories are discussed below.

3.1.2.1 Basic Safety Requirements. The purpose of CAS is to prevent vehicle-to-vehicle collisions in the event that safe vehicle headway is, for any reason, not maintained by the primary traffic control system. It must be implemented and operated independently of the primary system. The CAS must employ fail-safe principles such that a failure in the CAS will cause the system to revert to a safe state.

A word on "fail-safe" is in order here. The Fail-Safe Principle, as traditionally defined in the railroad signal and control industry, states that any failure or failures of the system shall not cause an unsafe condition. This is an ideal which is impossible to attain because there are always identifiable failures which can cause dangerous conditions to exist. In practice this principle means that if a system is to be acceptable, unsafe conditions must be sufficiently improbable to satisfy safety objectives.

The term fail-safe, as applied to the CAS, was first defined by Bendix early in the Morgantown project. This definition, in intent if not in exact words, has carried through to the present and has been influential in shaping the final CAS design.

> "No plausible failure or group of correlated multiple failures shall cause any part of the system to be placed in a posture which potentially hazards the life and limb of riders, operators, and awaiting passengers. The effects of multiple non-correlated failures

are considered if each failure goes undetected and leaves the affected part(s) of the system operational."

In addition to the single point failure concept, the above definition encompasses correlated failures and undetected noncorrelated multiple failures. Correlated failures are multiple failures which can result from a single primary failure or act. It is possible that any one of these component failures taken singularly can be detected as a failure and be safe, but in combination with one or more others it may be unsafe. Non-correlated multiple failures are included because a single failure can go undetected leaving the system operating satisfactorily. Over a period of time a second failure may occur which in combination with the first leaves the system unsafe.

3.1.2.2 Derived Safety Requirements

3.1.2.2.1 Phase II Specifications. The following requirements are contained in the System Specification and C&CS Specification Documents for Phase II. Although these are primary design requirements for the Phase II system, they are regarded as derived requirements relative to the CAS concept and the basic safety function of the CAS.

The C&CS shall have a collision avoidance capability independent of the primary point follower control system to protect vehicles against collisions because of interval violations, merge conflicts, and unverified switching. The collision avoidance capability shall be employed on the main guideway, on the acceleration and deceleration ramps (station merge/demerge ramps), on the station entry/exit ramps, and on the maintenance facility test loop. The collision avoidance capability shall be sized to assure that a safe stopping interval is maintained and to assure that a vehicle operating within the maximum vehicle position error shall not invoke emergency braking.

The collision avoidance equipment shall incorporate fail-safe design principles so that any single hardware element or component failure shall result in the removal of safe tone.

Interval Protection. The collision avoidance capability shall command emergency braking whenever the interval between vehicles becomes less than a safe value. A safe value is defined as the 3 σ maximum stopping distance of vehicles, referenced from vehicle position at loss of safe tone or on receipt of emergency stop command. These are as follows:

Nominal Car Speed, ft/s	Percent Grade	3 σ Max Stop Distance, Ft.
4	0	0
8	-10	24
	0	15
	+10	15
22	-10	75
	0	58
	+10	58
33	-10	136
	0	102
	+10	102
44	4.25	225
	0	216
	0.5	216

Merge Protection. The collision avoidance capabiity shall provide merge protection at each merge point in the system. This protection shall allow only one vehicle into a merge area. Any other vehicle entering the merge area shall be stopped by emergency brakes.

Switch Protection. The collision avoidance capability shall provide switch protection. A vehicle shall be stopped by emergency brakes if a verification of switchings is not received or if false verification is received.

3.1.2.2.2 Checked Redundancy. In Phase IA, the CAS consisted only of a single hardwired logic system to sense a safe vehicle headway violation and to turn the safe tone off under the trailing vehicle. In this arrangement, an undetected failure in the CAS could render the system inoperative and, thus, cause collision protection to be lost. In other words, it was not fail-safe. The inadequacy of this arrangement was identified in Bendix safety analyses; Bendix subsequently concluded that the CAS must be fail-safe and recommended that "checked redundancy" be employed to accomplish this.

The principle of checked redundancy employs checked redundant circuits to perform vital functions rather than non-redundant "fail-safe" circuits. railroad practice has allowed the use of checked redundancy in safety control. The checked redundancy principle is the use of two (or more) separate and distinct subsystems to perform the same safety function. Included is a failsafe comparing (checking) function so arranged that if the two subsystems do not agree, there results a restrictive decision producing a failure condition that is recognizable and safe. One of the requisites for safety is that the checking process be either a continuous one, or, at minimum, one which has a very small increment of time between checks. Each of these distinct subsystems may be so constituted that a single "frequent" type failure mode could cause it, in itself, to produce a dangerous condition were it not for the checking function.

Without the checking function, two failure, one in each branch, could cause an unsafe condition. These failures could occur at widely space time intervals, and the probability of this happening would be unacceptable.

With the checking function incorporated as part of the system, the two failure in the two branches could still cause a dangerous condition but only if they occurred within the small time period represented by the checking interval of the comparing function. If a single failure in either one of the of the branches occurred during this checking interval,

then the result would be a safe condition. Thus, the unsafe "event" for the checked redundancy principle is the occurrence of an unsafe-condition-producing failure in each of the checking time interval. For small intervals the probability of the unsafe event is very low and decreases as the interval of time decreases.

It is important that the separate failures be noncorrelated so that the probability of random events will apply. Care must be taken in the design so that multiple failures in the two redundant paths cannot be caused by a common transient environmental condition or else the two failures will occur at exactly the same instant and the comparing circuitry will not detect them. When considering checked redundancy, the comparing element must be fail-safe. It must be impossible for this comparing element to indicate agreement when there is none or when there is a failure in the comparing (checking) element itself.

Thus, the basic fail-safe requirement of the CAS translates into the derived requirement that it must employ checked redundancy. The following requirements are from the C&CS Specification. The station/guideway collision avoidance subsystem shall consist of magnets located on the vehicle, dual redundant presence detectors at each CAS presence detector location, presence detector electronics, and dual redundant paths to accomplish the collision avoidance block occupancy and safe tone control logic. One logic path shall be through the SCCS computers, and the other logic path shall consist of hardware collision avoidance logic circuitry. Collision avoidance shall be provided by control of a safe tone which in turn interfaces with a vehicle receiver and brake system. A disparity detector shall compare signals from each of the dual collision avoidance logic paths and shall deactivate a tone control device to indicate a failure when the two logic paths disagree. Indicators shall indicate which disparity detector caused the tone control device to deactivate.

Figure 3-1 presents the lower level derived requirements in functional block diagram form. The equipment performing the CAS logic functions to the left of the vertical dotted line need not be fail-safe in themselves.

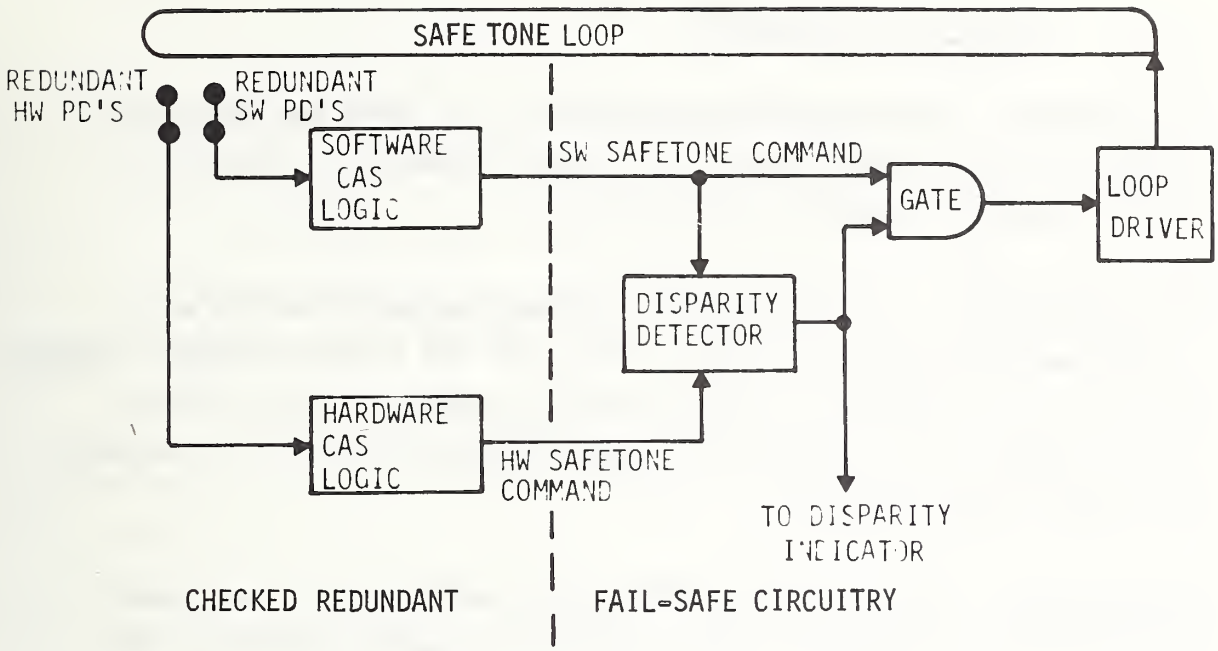


FIGURE 3-1. CAS FUNCTIONAL BLOCK DIAGRAM - DERIVED REQUIREMENTS

The fail-safe characteristic is obtained at the system level by the disparity detector, which compares the safe tone commands from the software and hardware CAS logic circuits and detects any disagreement caused by a failure or other anomalous condition.

The checked redundancy principle is employed only to the left of the dotted line. All circuitry to the right of the line is part of the comparator and must be fail-safe. In this equipment, plausible failure must not result in the safe tone failing ON. Failures which cause the safetone to fail OFF are acceptable from a safety stand point in that this mode of failure will stop any vehicle in that safe tone loop.

3.2 OPERABILITY

It does not automatically follow that because a system is safe, it is reliable. It is necessary to address the reliability of the CAS as a separate subject from its safety function. The CAS must be designed in such a manner that it does not stop vehicles unnecessarily when no potential hazard exists. The design must also facilitate system recovery by the operators and maintenance personnel after a CAS stop or a disparity. The following paragraphs present the CAS operability requirements.

3.2.1 Operating Requirements

The purpose of the following requirements is to limit the deleterious impact of CAS on system operation to those instances and locations where a potential hazard actually exists.

Operating Margin. The CAS must not command emergency braking when a safe operating headway exists - i.e., when the interval between leading and trailing vehicles is greater than 12.8 seconds (design interval of 15 seconds less allowance for vehicle position error of 1.1 seconds for each of two vehicles).

Reliability. The CAS must be sufficiently reliable such that there is no significant impact on system operations due to failure in the CAS. The probability of a safe tone being OFF when it should be ON must be no greater than 3.24×10^{-5} per hour.

Disparity Threshold. In order that the disparity detector does not respond to spurious signals and remove safe tone unnecessarily, a minimum time threshold must be specified. The hardware and software CAS signals must be in disagreement for a definite time duration to result in a CAS disparity. This requirement is also necessary to avoid generation of a disparity resulting from the fact that the hardware CAS is time continuous, whereas the software CAS operates on a discrete sampling rate resulting in momentary disagreement for every input signal change of state. For Morgantown, disagreement must persist for 0.5 seconds, and the safe tone must be turned off within 1.0 second.

CAS Zones. It is both undesirable and unnecessary to stop all vehicles in the entire system when a single CAS disparity occurs. To limit the amount of guideway closed by a CAS disparity, safe tone loops should be logically grouped into CAS Disparity Zones such that in most circumstances the safe tones are removed only in one zone. The current MPM system has 29 such zones.

3.2.2 Recovery Requirements

In the usual case of a safe headway violation, no particular recovery requirements are levied against the CAS. The CAS does not normally assume an anomalous or abnormal state that requires corrective action. It is only necessary to ascertain the cause of the headway violation, to rectify or otherwise neutralize the problem, and to get the vehicles moving again. This does not require a special role from the CAS.

In the case of a CAS disparity, the CAS is involved in the recovery procedure. The CAS is required to have disparity monitors which will indicate which safe tone loop is associated with the disparity. The object of this requirement is to aid in identifying the cause of the disparity, (i.e., which pair of PDs and/or vehicle were involved, or what piece of CAS equipment failed). The capability must be provided to override the disparity temporarily, allowing the guideway to be cleared by bringing vehicles into the stations one at a time. Means are also required to clear the disparity state and to turn off the disparity monitors once the original cause of the disparity has been identified and rectified.

In certain circumstances after a CAS stop, it is necessary to reconfigure the information stored in the CAS in order to bring the system up. Manual means--namely, presence detector hits (both hardware and software) and switch verification signals--must, therefore, be provided to simulate normal inputs to the CAS. These capabilities are also required for maintenance purposes, and the manner of providing them is specified further in Section 3.3.

3.3 MAINTENANCE

When performing maintenance, tests, or troubleshooting involving the CAS, it is necesary to have some means of providing any desired set of inputs to CAS other than use of actual vehicles on the guideway. The Morgantown specifications require these functions to be provided

on a "CAS Test and Maintenance Panel" (T&M Panel), one located in each station. Each panel must provide the following:

1. A continuous display of the safe tone status in each station control zone.

2. The capability to simulate presence detector inputs.

3. The capability to simulate switch verification signals.

4. Capability to display stop tone status for Maintenance, Engineering, Towers and Med Center Stations.

Each panel must be designed so that the location of the devices on the panel are labeled and correlate to the topography of the zone being controlled. The panel must be easily removable for repair without affecting the operations of the system. The disparity override capability specified in Section 3.2 and used to aid system recovery is also a requirement for maintenance operations.

4. CAS DESIGN

The Collision Avoidance System (CAS) currently implemented in the Morgantown People Mover (MPM) is based upon design concepts selected by design trade studies performed by the Jet Propulsion Laboratory during 1971. While the design has been refined for improved safety, reliability, and maintainability, the basic concept has been retained. The CAS operates in conjunction with, but independently of the normal vehicle control system. Under normal circumstances the CAS protection is present but "unseen" (i.e., the CAS does not affect normal operations). However, if for any reason the primary control system should fail to provide safe vehicle separation, the CAS will stop vehicles as required to avoid the possibility of collision.

4.1 DESIGN CONCEPTS

The CAS design adopted for the MPM is based upon a block occupancy concept. The guideway is divided into discrete blocks each of which may not be occupied by more than one vehicle. Since the single vehicle occupancy rule must be enforced under all conditions, a vehicle which enters a block behind an occupied block is commanded to stop.

The block occupancy concept has been employed extensively in railroad applications technology. The block concept has been proven very effective through a century of application to systems ranging from manual to fully automatic. While the block occupancy concept is derived from railroad technology, the MPM block occupancy status is obtained in a unique manner. Railroads continuously monitor block occupancy using a multiplicity of steel wheels and axles to complete an electrical circuit between the two rails at isolated track segments.

The MPM uses rubber tired vehicles running on concrete guideway, hence, lacks a ready-made detection system that can be monitored on a continuous basis. Continuous detection was considered during Phase I but no scheme

was felt to provide sufficient reliability when applied to MPM. This is largely due to the fact that a single vehicle with rubber tires cannot provide the multiply redundant shorting paths inherent in railway systems. Trade studies performed led to selection of a check in -check out detection system. This system consists of vehicle presence detectors installed at block boundaries along the guideway. The presence detectors are activated by permanent magnets attached to the vehicles. When a presence detector is activated by a passing vehicle, the block ahead is set occupied and the block behind is set clear. Note that a vehicle always checks into one block when it checks out of another.

Vehicles are prevented from entering occupied blocks by a scheme which results in maximum rate braking if a vehicle enters a block while the block ahead is occupied. This is achieved by requiring a vehicle to apply emergency brakes any time the vehicle does not receive a safe-to-proceed command from the CAS. The safe-to-proceed command (safe tone) is provided by a 10.2 kHz carrier modulated at 50 Hz transmitted via safe tone loops embedded in the guideway. The safe tone behind an occupied block is always off, hence, a vehicle will apply emergency brakes any time the block ahead is occupied. In the original design (Phase IA) safe tones were normally-on. Most safe tones were only turned off behind occupied blocks. Safety analysis at the end of Phase IA and beginning of Phase IB concluded that normally-off safe tones were required at switches and merges. No significant advantage could be identified for providing normally-off safe tones elsewhere.

Switch guard loops are provided to stop vehicles which fail to switch properly when a switch command is received. Switching protection is provided by means of a normally-off safe tone just past each switch command loop. When a vehicle receives a switch command, the vehicle switches (if necessary) then transmits a switch verification signal to verify that steering is being performed on the correct side. When switch verification is received, the switch guard safe tone is turned on. In the Phase IA design the switch guard was normally on and was turned off as the vehicle approached the switch. In Phase IB the logic was modified to turn the safe tone off upon vehicle departure from the switch zone. Thus, switch guards are normally off. The advantage

of a normally-off safe tone is that a "silent vehicle" (a vehicle which fails to activate presence detectors) will be stopped. If the safe tone were normally on, a silent vehicle would not have switch guard protection.

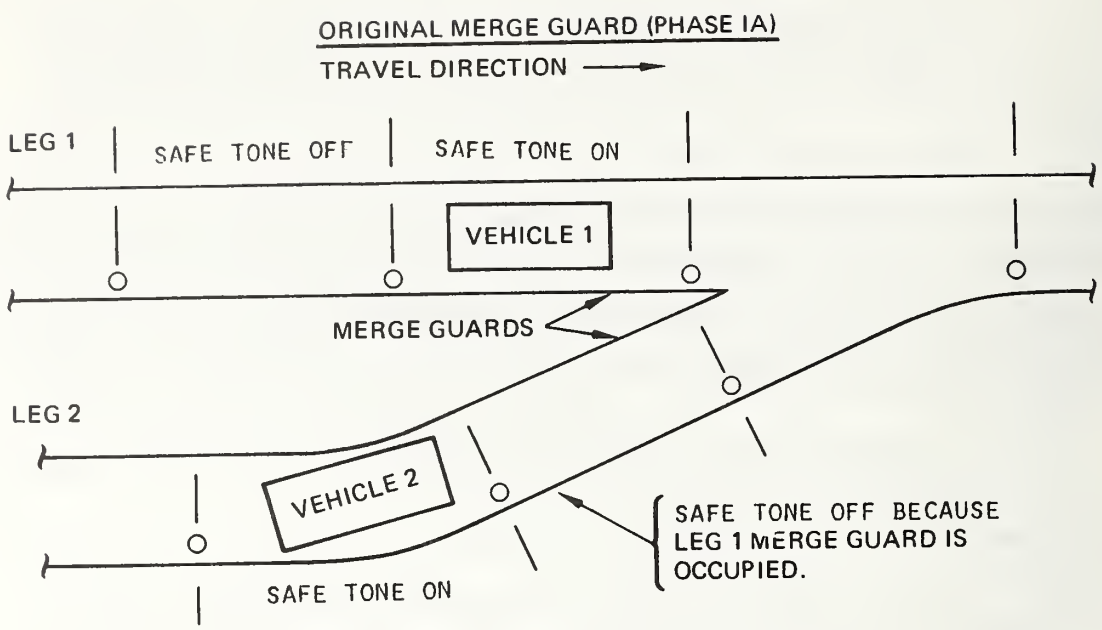
Merge guard loops provide protection against collisions at merge points. The Phase IA CAS provided merge protection on the basis of block occupancy. A safe tone in a merge area would be off if either the adjacent block or the block ahead was occupied. This design had two problems:

1. A silent vehicle could enter a merge area and would be unprotected if it stopped.

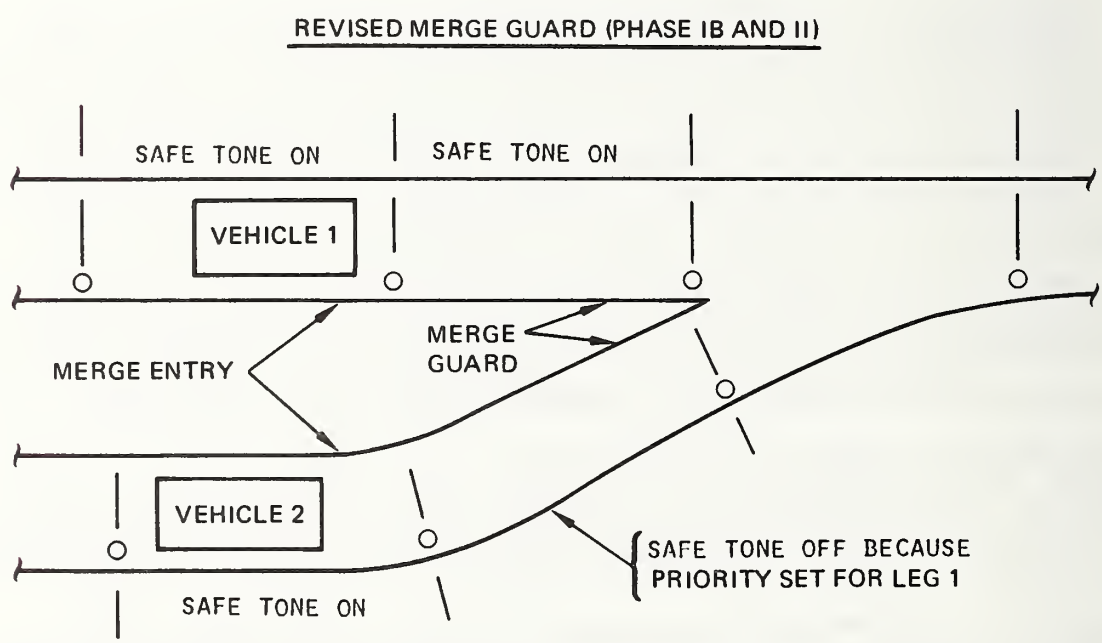
2. If two vehicles entered a merge area from opposite legs, both vehicles would be stopped and neither vehicle could be restarted.

Silent Vehicle. The first problem presented a potential safety hazard. If a vehicle traveling along the guideway were to lose its magnet (or become silent for any reason) the vehicle would be protected because the last block it occupied would not be cleared. Thus, a safe tone would remain off behind the vehicle leaving the vehicle well protected in the guideway section within which the failure occurred. However, this protection would be lost if the vehicle reached a merge area and would not be regained beyond the merge area because vehicles could enter from the other leg. This potential hazard is avoided by use of normally-off safe tones which guard merge points. The safe tone guarding a merge area (merge guard) is off unless either the merge guard or the preceding block is occupied. Thus, a vehicle must indicate its presence in order to proceed; hence, a silent vehicle would be stopped.

Merge Operability. The second problem degraded system operability since any merge conflict would lock up both legs. This problem and the solution are illustrated in Figure 4-1. The problem has been eliminated by substituting a priority latch for block occupancy in merge guard logic. A priority latch is set for a given leg when a vehicle arrives. The latch remains set for that side until the opposite side gains priority. The opposite leg cannot gain priority until all blocks on the first leg have been cleared,



A merge guard is off whenever the other leg is occupied. Leg 1 merge guard will go off when vehicle 2 enters leg 2 merge guard.



Vehicle 1 entered merge first hence leg 1 has priority. Leg 2 cannot gain priority until vehicle 1 clears the leg 1 merge guard.

FIGURE 4-1. MERGE PROTECTION

(i.e., not until the first vehicle clears the merge area). Thus, two conditions must be satisfied to obtain priority: 1) a vehicle must be arriving and 2) the opposite leg must be unoccupied. The merge

guard safe tone for each side is always off if the opposite side has priority. Even when priority is favorable, a merge guard is off unless a vehicle is arriving. This prevents a silent vehicle from following a normal vehicle through a merge guard. Thus, the three safety and operability criteria are met:

1. A vehicle will be stopped if it enters a merge area when the opposite leg is occupied.

2. A silent vehicle will be stopped.

3. A vehicle will not be stopped by arrival of a second vehicle. After the first vehicle clears the merge area, the second vehicle will obtain priority and can be restarted The safety study performed at the start of Phase IB identified two other areas of concern.

The safety study performed at the start of Phase IB identified two other areas of concern.

1. Block occupancy status was limited to a single vehicle. If two vehicles were to enter a single block, the block would be cleared when the first vehicle departed leaving the second vehicle unprotected. "Slide-through" (entry of second vehicle in occupied block) is very improbable, but the consequences are too serious to tolerate.

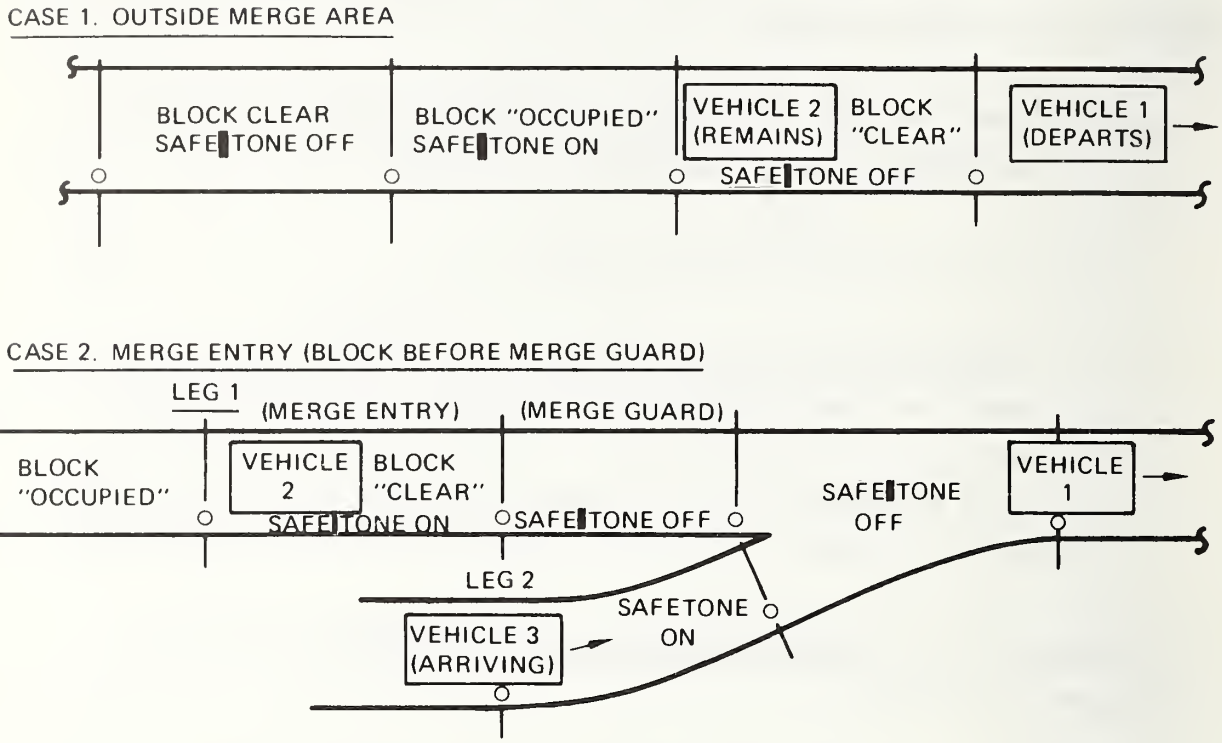
2. The Phase IA CAS was a single thread system, hence, vulnerable to certain single point failures.

Slide-Through. Conceptually, two alternatives were available to correct the slide-through problem:

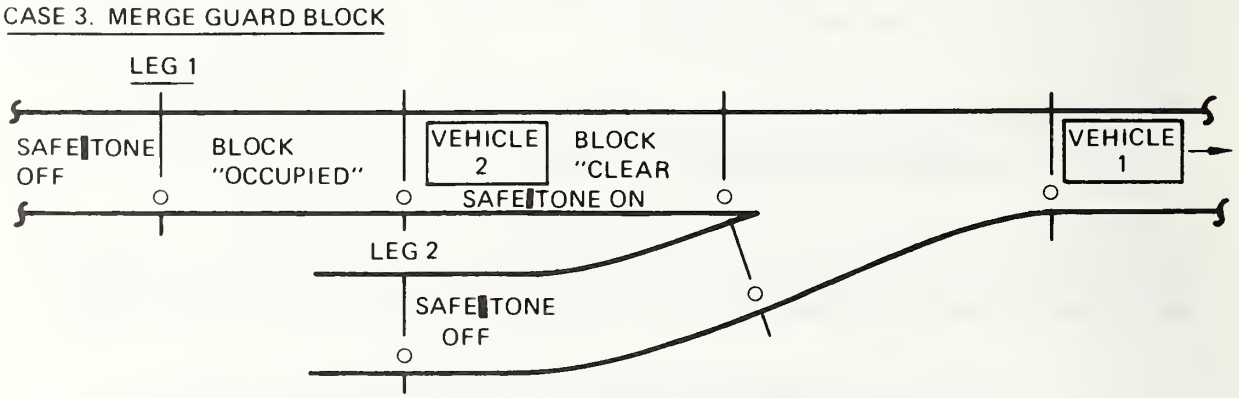
1. Avoid clearing the block when the first vehicle departs, or

2. provide protection which remains when the block is cleared by departure of the first vehicle.

The second alternative was selected. Slide-through protection is provided by not clearing the departed block when an occupied block is entered. Thus, trailing vehicles cannot reach the departed block. Slide-through protection is illustrated in Figure 4-2.



Vehicle 2 is protected from behind as in case 1. Leg 1 does not have merge priority because the block containing vehicle 2 is "clear". However, vehicle 2 is physically clear of the merge, hence, is not in danger of a collision with vehicles arriving on leg 2. Any vehicle which arrives on leg 2 will gain priority. Vehicle 2 cannot advance past the merge guard which remains off until block occupancy is corrected.



The merge guard on leg 2 is off because leg 1 retains priority as long as the leg 1 entry block is occupied. This would also be true of a slide-through in the next block.

FIGURE 4-2. SLIDE-THROUGH PROTECTION

Up to the time of this report, no slide-through has occurred in the MPM system. This is not surprising since the blocks are of sufficient length to avoid slide-through even given multiple concurrent worst case conditions. Nevertheless, the system is designed to protect against such an event.

Dual CAS Requirement. The single thread CAS was considered inadequate because it was found to be vulnerable to single point failures which were not fail-safe. For example, false activation of a presence detector could cause false checkout of an occupied block. If this occurred, the vehicle would be stopped since the safe tone would be removed by the apparent occupancy of the block ahead. Furthermore, the block containing the vehicle would be cleared removing its protection. (The safe tone behind would be turned on.) Although the control software would stop trailing vehicles, this failure mode violates the ground rules for a fail-safe CAS; hence, a resolution was necessary. Alternatives considered included continuous detection, mechanical detection, and various forms of redundant CAS. The first two alternatives were rejected due to cost, reliability, and developmental risk considerations. Furthermore, the redundant CAS reduces vulnerability to failures other than detection.

The redundant CAS selected consists of a hardware CAS and a software CAS each with its own presence detector inputs. Originally, different presence detector types were considered for the two CAS systems, but reed relays were selected for both due to superior reliability. The outputs of the hardware and software CAS are compared. If any disparity is found to exist longer than an operating tolerance (nominally 500 ms), the safe tone carrier signal is removed for all safe tones in the vicinity (CAS disparity zone). This is a checked system with automatic shutdown. However, it is commonly referred to as a checked redundant CAS in that a vehicle will be stopped if either side computes an off value for the corresponding safe tone. The software CAS removes the safe tone directly whereas the hardware CAS creates a disparity if not in agreement with the software. A disparity removes all safe tones from the affected CAS zone. A functional diagram of the Dual CAS is provided in Figure 4-3.

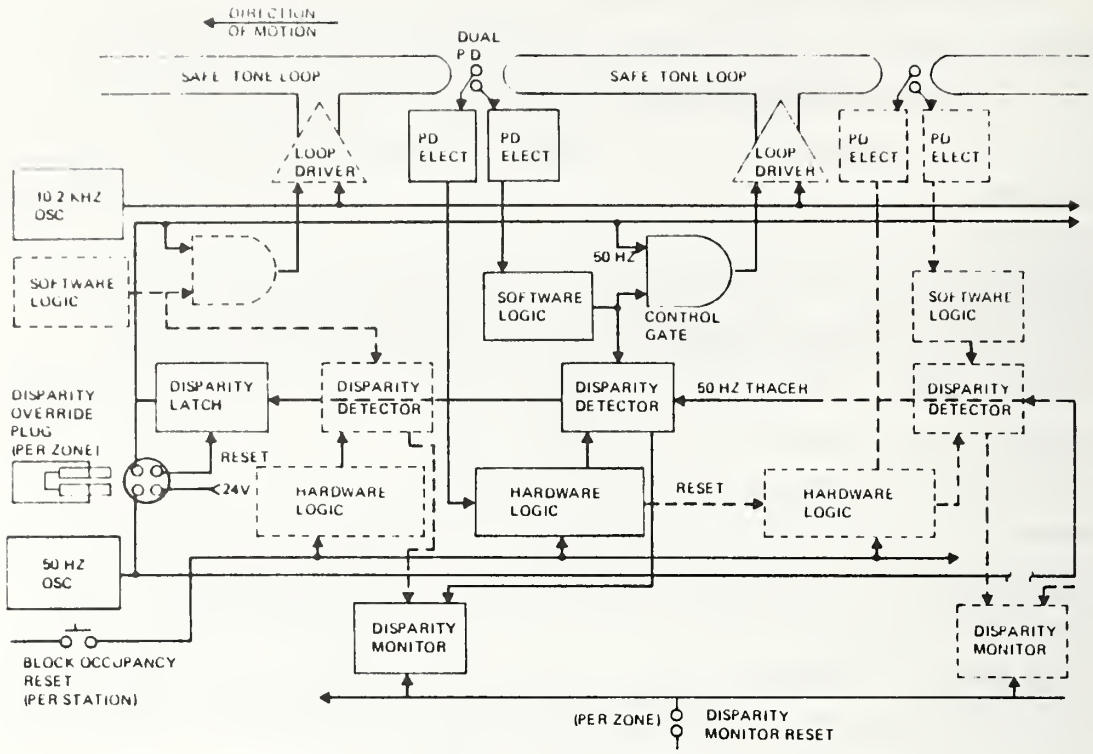


FIGURE 4-3. CAS FUNCTIONAL DIAGRAM

Disparities are deliberately created to stop vehicles in three situations:

1. Slide-through at handover

   The hardware CAS does not provide slide-through protection at a station boundary (handover point). This is because the hardware CAS for one station does not receive block occupancy data for a block in the next station. The software does provide slide-through protection at handover using block occupancy data transmitted between stations via the central computer. As a result, a slide-through at handover would create a disparity since the hardware would allow the preceding safe tone to turn on while the software would not.

2. False switch verification

The software CAS receives all switch verifications without regard to block occupancy. If a verification is received when the corresponding block is clear, the software turns on a normally-off safe tone thereby creating a disparity and removing all safe tones in the zone. Thus, all vehicles are stopped before reaching the switch.

3. Steering runout

Some sections of guideway have steering rail on one side only. If a vehicle approaches one of these areas while steering on the wrong side, it will activate a runout switch mounted on the guiderail. The switch intentionally causes a false hit on a software PD ahead thereby removing the safe tone under the vehicle and creating a disparity. This provision was added during Phase II without any impact upon the CAS design.

The above three cases involve failures believed to be sufficiently remote to rely upon single thread CAS protection.

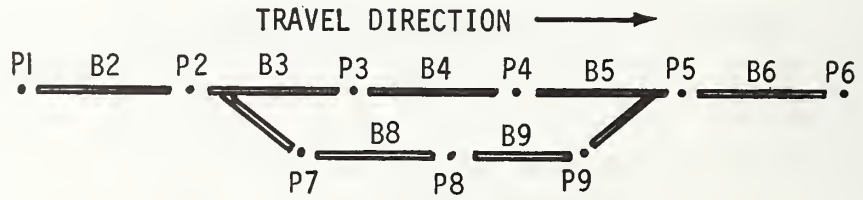
4.2 DESIGN TECHNIQUE

The following paragraphs discuss specifics of CAS logic, physical layout, and CAS reset capabilities.

4.2.1 CAS Logic Equations

The CAS logic is expressed in terms of Boolean expressions and equations. Boolean expressions are used to set block occupancy, priority latches, and switch latches. Boolean equations are used to maintain safe tone status.

4.2.1.1 Block Occupancy Expressions. Block occupancy is determined by monitoring presence detector (PD) activation. All segments of the MPM guideway are unidirectional since the system does not allow reverse movement. Therefore PD activation always indicates movement in the forward direction - the block behind is cleared and the block ahead is set occupied. Block occupancy is latched. Once set, a block remains occupied until the departure PD is activated. Once cleared, the block remains unoccupied until the arrival PD is activated. Block occupancy expressions for the following guideway layout illustrate main guideway, merge, and demerge situations.



Block	Set	Clear
B2	P1	$P2 \cdot \overline{B3}$
B3	P2	$P3 \cdot \overline{B4} + P7 \cdot \overline{B8}$
B4	P3	$P4 \cdot \overline{B5}$
B5	P4+P9	$P5 \cdot \overline{B6}$
B6	P5	P6
B8	P7	$P8 \cdot \overline{B9}$
B9	P8	$P9 \cdot \overline{B5}$

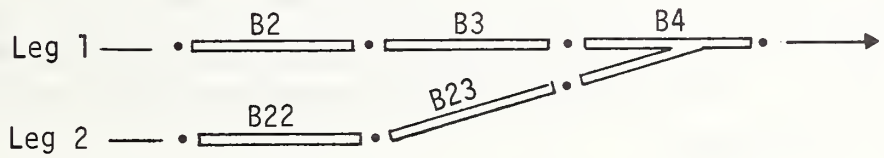
The expressions for B2, B4, B8 and B9 are typical for most main guideway blocks. These blocks are set when the entry PD is activated and cleared when the exit PD is activated if the block ahead is clear. (P2 $\overline{B3}$ means PD2 is activated and block 3 is clear.) The block is not cleared if the block ahead is occupied when the PD is activated. This provides slide-through protection as discussed in Section 4.1. Note that the

"clear" expressions must be evaluated before the "set" expressions. Otherwise, B2 could never be cleared since B3 is always set occupied when P2 is activated. The logic for B3 is typical for a demerge. The block is set by a single entry PD and cleared by either of two exit PDs. (The expression P3•B4 + P7•B8 means "P3 activated and B4 clear" or "P7 activated and B8 clear".)

The logic for B5 is typical for a merge. The block is set by either of two entry PDs and cleared by a single exit PD.

The logic for B6 is typical for two cases: (1) there is no block ahead; or (2) its status is unknown. The first case occurs in channels. CAS protection is not provided between berths in channels because insufficient space is available between berths and channel speed is low enough (4 ft/s) to preclude hazards arising from collision. Block occupancy is only maintained for one block ahead of the safe tone which guards entry to the rear berth. The second case occurs at the boundary between stations. The hardware CAS for a station does not have the block occupancy for the first block in the next station, hence, does not provide slide-through protection at handover. The software CAS provides the necessary slide-through protection at handover as discussed in Section 4.1.

4.2.1.2 Priority Latch Expressions. A priority latch is used to give an occupied leg of a merge "right of way" over the opposite leg. The "right of way" (priority) is retained until the first leg is cleared and the other leg becomes occupied. The following example is typical for merges on the main guideway.



The priority latch is set for leg 1 when the following expression is satisfied: $(B2+B3)\bullet(\overline{B22}\bullet\overline{B23})$. That is, a vehicle must be entering from leg 1 (B2 or B3 must be occupied) and leg 2 must be clear (B22 and B23 must be clear). The priority latch is cleared (set for leg 2) when the expression $(\overline{B2}\bullet\overline{B3})\bullet(B22+B23)$ is satisfied. This occurs when a vehicle enters on leg 2 after leg 1 clears.

A single priority latch is used for a merge. This is a fail-safe design since it is not possible to give both legs priority at the same time. The symmetry of the set and clear logic for a priority latch creates a temptation to replace the set and clear logic by a single Boolean equation:

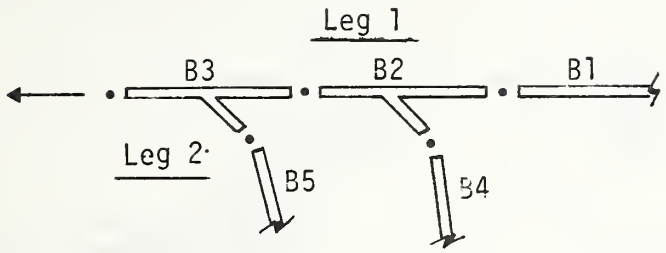
$$PL = (B2 + B3)\bullet(\overline{B22}\ \overline{B23}).$$

This approach was used in the initial software design until it was pointed out that the resulting expression for resetting the priority latch (giving priority to leg 2) would be:

$$\overline{PL} = (\overline{B2}\bullet\overline{B3}) + (B22 + B23).$$

This would violate a ground rule for priority latches: priority cannot be rescinded for an occupied leg. Once granted, priority must be retained until the leg is clear.

For the preceding example the merge guard safe tones would be located at B3 and B23. Priority is granted at the merge entry block (e.g., B2 for leg 1) so that the merge guard will be on when the vehicle enters the block. In more constrained areas (primarily channel merges) one leg cannot obtain priority until the merge guard block is entered. Special provision for such cases is discussed in Section 4.2.1.4. Priority for the other leg must sometimes be granted for two merge entry blocks. In the following example merge guard safe tones are located at B2 and B5.



B1 and B4 are entry blocks for leg 1. B5 is entered from a berth, hence, priority cannot be granted to leg 2 until a vehicle enters B5. For this case priority is given to leg 1 (priority latch set) by

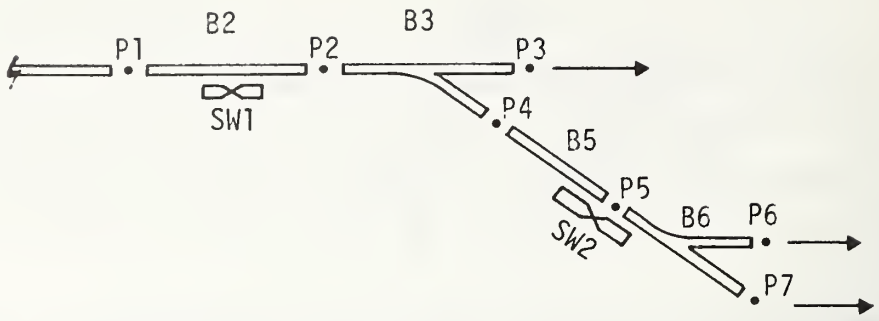
(B1+B3+B2) B5.

Priority is given to leg 2 (priority latch cleared) by

B5 (B1 B4 B2).

Priority logic can be summarized as follows: Priority is granted to a given merge leg if any of its blocks (merge guard or entry) is occupied and no block (guard or entry) on the opposite leg is occupied . Once obtained, priority is retained until granted to the opposite leg.

4.2.1.3 Switch Latch Expressions. A switch latch is set when a vehicle provides switch verification. The switch latch is cleared when the vehicle departs or when another vehicle arrives. The set logic for the hardware CAS differs from that for the software CAS. If switch verification is received from an unoccupied block, the switch latch will be set for the software CAS but not for the hardware CAS. In this case the software will turn on the switch guard loop to create a disparity. This prevents system operation with false switch verification provided by a failure in the station electronics. In the following example SW1 and SW2 are switches with corresponding verification signals, SV1 and SV2, and switch latches, SL1 and SL2.



Switch Latch	Set (S/W)	Set (H/W)	Clear
SL1	SV1	SV1•B2	P1+P3+P4
SL2	SV2	SV2•(B5+B6)	P4+P6+P7

The switch guard loop will normally be located in a position corresponding to B3 for SW1 and to B6 for SW2.

4.2.1.4 Safe Tone Equations. Safe tone status is set as specified by Boolean equations involving block occupancy, priority latch, and switch latch status. Five basic types are used -- normally-on, switch guard, merge guard, combined switch/merge guard, and always on.

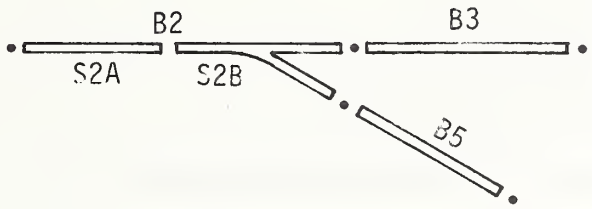
Normally-On Safe Tone Equations. Most safe tones are normally on. A normally-on safe tone is on unless the block ahead is occupied.

$$S_n = \overline{B}_{n+1}.$$

This is the simplest and most common safe tone equation. Occasionally (at branch points) two blocks must be clear. The form then becomes:

$$S_2 = \overline{B}_{n1} \cdot \overline{B}_{n2}.$$

In the following example the safe tone for B2 is divided in two parts, S2A and S2B. S2B is the switch guard. Switching occurs while vehicles are on S2A.



For this case S2A = $\overline{B3} \bullet \overline{B5}$. Note that all normally-on safe tones are on when the guideway is clear. This is not true of switch guard and merge guard safe tones.

Switch Guard Equations. Whenever a vehicle receives a switch command, the vehicle is required to verify that switching has been successfully completed. The verification indicates that the vehicle is currently steering on the commanded side. Lack of verification indicates that the vehicle did not properly complete the switching sequence.

Switch guard safe tones are used to stop vehicles which fail to verify switching. The safe tone equation for a switch guard at a demerge location has the following form:

$$S_n = SL_m \bullet \overline{B_{n1}} \bullet \overline{B_{n2}}.$$

The safe tone is normally off since the switch latch is normally off unless a vehicle is present.

Switch commands are also issued after most merges. This is because a guide rail is not usually provided on the side opposite the normal steering side. Therefore, vehicles merging from one side must switch before the guide rail terminates. For this case the switch guard equation is:

$$S_n = SL_m \bullet \overline{B_{n+1}}.$$

Merge Guard Equations. Merge guard safe tones protect merging vehicles in three ways. A vehicle is stopped by the merge guard for any of the following conditions:

1. Block ahead occupied.

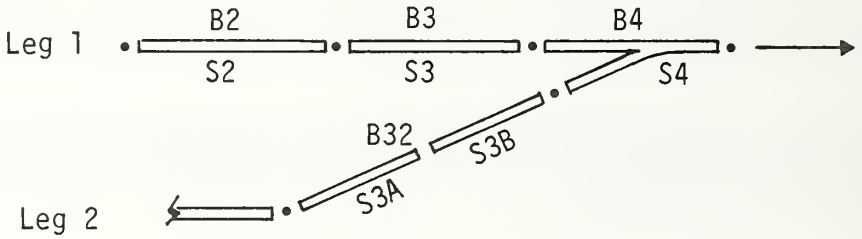
2. Opposite leg of merge occupied.

3. Vehicle fails to activate merge entry PD.

The expression for a merge guard safe tone is the logical product of three terms, each providing protection against one of the above conditions:

(Blocks ahead clear) . (Priority granted) . (leg occupied).

The first term is the same as the expression for a normally-on safe tone. The second term is a priority latch. The third term requires that the merge entry or merge guard be occupied. In the following example the priority latch (PR) is set for leg 1 given $(B2+B3)\bullet\overline{B32}$. Priority is given to leg 2 (PR cleared) for $(\overline{B2}\bullet\overline{B3})$ B32.



Leg 1 has sufficient space for normal treatment: B2 is the merge entry block; B3 is the merge guard block. The equation for the leg 1 merge guard safe tone is given by:

$$S3 = \overline{B4}\bullet PR\bullet(B2+B3).$$

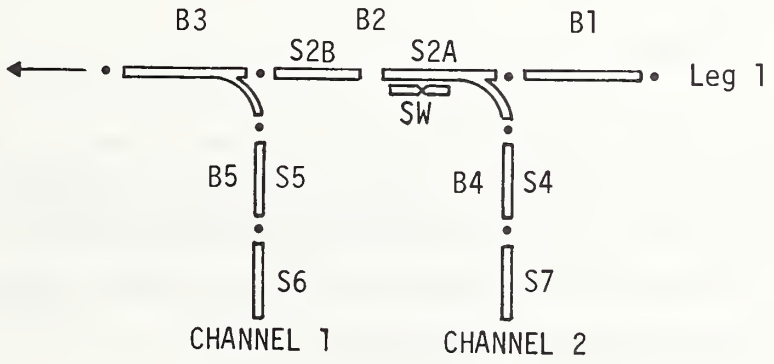
Thus, S3 turns on when a vehicle enters B2 and remains on until the vehicle enters B4. (Note that if S3 were not turned on for B2 the vehicle would momentarily lose safe tone upon entering B3. This would stop the vehicle since loss of safe tone is irrevocable - the resulting stop command remains in force until the vehicle is commanded to restart).

Leg 2 illustrates the approach used when space constraints do not allow use of an entry block. The safe tone for block B32 is split into two safe tone loops with equations:

$$S3A = \overline{B4}$$
$$S3B = \overline{B4} \bullet \overline{PR} \bullet B32.$$

The safe tone loop for S3A need only be long enough to allow time for S3B to be updated before a vehicle reaches S3B. The loop for S3B needs to be long enough to provide an adequate stopping margin without obstructing leg 1.

Combined Merge/Switch Guard Equations. It is sometimes necessary for a single safe tone loop to provide combined merge guard and switch guard protection. This occurs in constrained areas such as station channel merge areas. In the following example S5 is the merge guard for channel 1. S2A and S2B both serve as merge guards for vehicles entering from leg 1 or from channel 2. S2B also serves as a switch guard.



$$S2A = \overline{B3} \bullet PR \bullet (B2+B1+B4)$$

$$S2B = \overline{B3} \bullet PR \bullet B2 \bullet SL$$

B1 and B4 are not included in the equation for S2B because S2B need not be turned on until B2 is occupied. B2 could also be omitted since B2 must be occupied before switch latch, SL, can be validly set. This simplification is sometimes used.

Always-On Safe tones. In the preceding example S6 and S7 are channel berthing safe tones. These safe tones are always on because station berths are too closely spaced to allow for CAS operating margins. Operation without an independent CAS is allowed within berthing areas because vehicle speed is limited to 4.4 ft/s. (This is 3 miles per hour - a moderate walking speed.) The vehicles are designed to withstand a 4.4 ft/s collision without passenger injury or vehicle damage. Furthermore, vehicle control in a berthing area does not allow a vehicle to depart a berth unless the berth ahead is completely clear. In the preceding example the forward berth is not considered clear if either the berth or B5 is occupied. Similarly, the next berth back is not clear if that berth is occupied or if a vehicle is between that berth and the forward berth.

The presence of an always-on safe tone is necessary for the CAS layout in the preceding example. The safe tone equation for S5 is:

$$S5 = \overline{B3} \bullet \overline{PR} \bullet B5.$$

This is operational because the always-on safe tone, S7, extends a short distance into block B5. When a vehicle first enters B5, S7 provides a safe tone while the CAS processes the PD activation and turns on S5. The distance that S7 extends into B5 is small, hence does not adversely affect the stopping margin in B5.

4.2.2 CAS Layout

The guideway layout of CAS blocks must satisfy safety and operability constraints. Operability requires the layout to allow vehicles to operate without stopping as long as minimal headway requirements are satisfied. Safety requires the enforced vehicle separation to exceed worst case stopping distances.

The following sections provide theoretical considerations, layout procedures used for MPM, and some practical considerations for CAS layout.

4.2.2.1 Theoretical Considerations. Theoretical considerations for CAS layout were discussed in a report from APL dated August 1971.[1] The report derives layout constraints and discusses optimization of block lengths. The results of the report have limited applicability to the final Morgantown CAS due to significant conceptual differences. (The proposed system provided combined collision avoidance and speed control. Speed control information was to be passed to the vehicle on the basis of the number of clear blocks ahead.) The resulting block length was much smaller than required for the single aspect system now in use. While the results are not applicable to the current CAS, the constraints are applicable when properly adapted to the Morgantown configuration.

Applicable layout constraints can be expressed in terms of the following definitions:

1. Headway

   H = Nominal time between adjacent vehicles.

2. Minimum Headway

   T = Headway - Design Tolerance.

3. Command Speed

---

[1] Control Concepts for the Morgantown Project, APL/JHU CP 007 TPR 022, August 1971.

V = Nominal vehicle speed at start of safe tone.

4. Stopping Distance

D(V) = Worst case stopping distance.

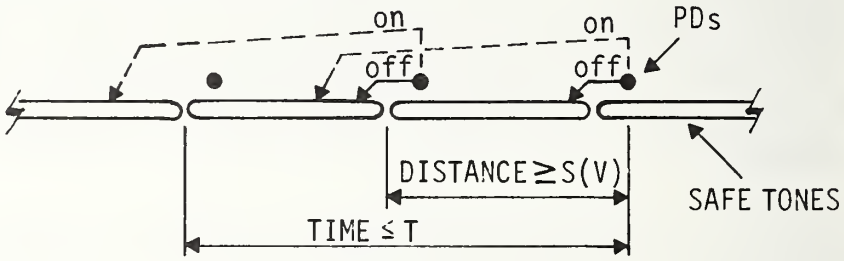
5. Minimum Separation

S(V) = D(V) + Vehicle Length + Safety Margin.

Two basic constraints apply:

1. The distance from the start of a safe tone to the PD that turns on the preceding safetone (and turns this one off) must at least equal the minimum separation, S(V).

2. The nominal travel time from the start of a safe tone to the PD that turns it on (and the next safe tone off) must not exceed the minimum headway, T.



In constant speed zones with no switches or merges it is best to use fixed length blocks. PDs should be separated by the block length. The block length may exceed neither VT - S(V) nor VT/2. Cost is minimized by using the maximum allowable length, L, where

$$L = \begin{cases} VT/2 & \text{if } VT/2 \geq S(V) \quad (1) \\ VT - S(V) & \text{otherwise} \quad (2) \end{cases}$$

Case 1. Headway Constraint Dominant.

If $VT/2 \geq S(V)$ proceed as follows:

1. Lay out safe tones of length $L = VT/2$.

2. Place PDs at safe tone boundaries.[1]

Case 2. Separation Constraint Dominant.

If $S(V) > VT/2$ proceed as follows:

1. Lay out safe tones at length $L = VT - S(V)$

2. Place a PD at distance $S(V)$ past the end of each safe tone.

Table 4-1 lists maximum block lengths for a 15.5 foot vehicle with a 0.5 foot safety margin and a 2-second headway tolerance. The listed stopping distances are 3 σ values for a Morgantown vehicle on level grade. The applicable constraint (case #) is also shown.

TABLE 4-1. MAXIMUM BLOCK LENGTHS

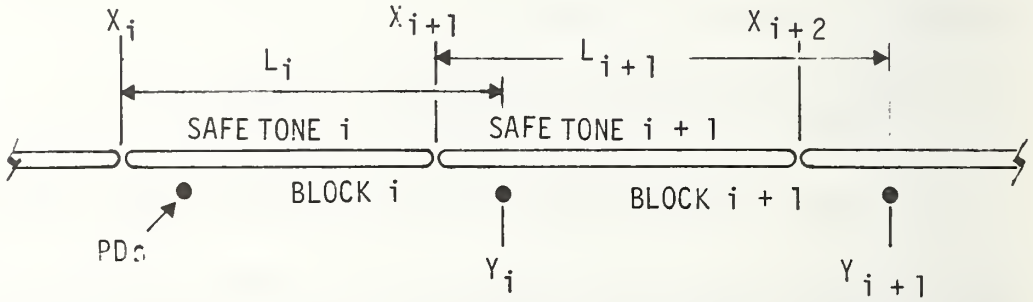
V	D(V) (feet)	S(V) (feet)	H(sec)[2]	Maximum Block (ft)	Case #
4 F/S	8	24	16	28	
			15	26	1
			12	16	
			10	8	2
			9	4	
			8	0	
8 F/S	15	31	16	56	
			15	52	1
			12	40	
			10	32	
			8	15	
			6	0	2
22 F/S	58	74	16	154	
			15	143	1
			12	110	
			10	88	
			8	58	
			5.4	0	2
33 F/S	102	118	16	231	
			15	214	1
			12	165	
			10	132	
			8	80	
			5.6	0	2
44 F/S	216	232	16	308	
			15	286	1
			12	208	
			10	120	2
			8	32	
			7.3	0	

[1] Theroetical position. For installation the physical position is offset to allow for the offset between a vehicle's magnet and safe tone antenna. (See Section 4.2.2.3)

[2] A theoretical minimum headway is included for each speed but is unattainable because zero length blocks would be required. These headways can only be achieved by reducing the headway tolerance or stopping distance.

When the headway constraint dominates (case 1), the safety margin exceeds the minimum. When the separation constraint dominates (case 2), the minimum safety margin applies, and an operating margin is available in addition to the headway tolerance.

The preceding equations do not apply to speed transition zones. Constraints can be expressed in terms of safe tone boundaries (X_i), block boundaries (Y_i), enforced separations (L_i), and nominal travel times (T_i) defined by the following diagram.



T_i is the nominal travel time from X_i to Y_{i+1} (i.e., travel from the start of a safe tone to the end of the controlling block).

The following constraints apply:

1. $L_i \geq S(V)$ where V = nominal velocity at X_i.

2. $T_i \leq T$.

3. $Y_i \geq X_{i+1}$.

Constraint 1 assures safety while 2 and 3 assure operability. Constraint 2 allows for any vehicle headway within design tolerance. Constraint 3 prevents a vehicle from removing its own safe tone.

The above constraints are applicable to all cases. For example, constant speed case 1 is obtained by setting $Y_i = X_{i+1}$ and using a fixed block length with $T_i = T$. Case 2 is obtained by setting $L_i = S(V)$ and $T_i = \frac{2S(V)}{V}$.

Blocks may be laid out in a speed transition zone by the following procedure starting with an initial postion (X_i) which is the end of the last safe tone in the constant speed zone.

1. Advance the nominal distance traveled in time T. Place a PD at this position (Y_{i+1}).

2. Move back to a position X such that $Y_{i+1}-X = S(V(X))$ (i.e. a position at which the velocity allows a minimum separation equal to the distance of the PD). This can be done iteratively or graphically.

   Set $X_{i+1} = \begin{cases} X & \text{if } X \leq Y_i \\ Y_i & \text{otherwise} \end{cases}$

   where Y_i = Position of PD controlling safetone i-1.

3. Increment i.

4. Repeat steps 1-3 until complete.

This procedure lays out blocks with maximum allowable length. Adjustments can be made to meet constraints imposed by station boundaries, merges, etc., by advancing less distance than allowed in Step 1.

The minimum allowable advance is S(V) + d where d, the minimum acceptable length for a safe tone, must be large enough for a vehicle to detect a loss of safe tone even if adjacent safe tones are on. In the Morgantown system step 2 always gives a value $X - Y_i$ hence $X_{i+1} = Y_i$. This would not be true for shorter headway in a downward speed transition nor in high and low speed zones.

Figure 4-4 illustrates a layout obtained by applying the above procedure to a section of guideway containing speed transition starting at 44 ft/s and terminating at 4 ft/s. The example allows a 10-second minimum headway, hence, would be operable for a 12-second nominal headway.

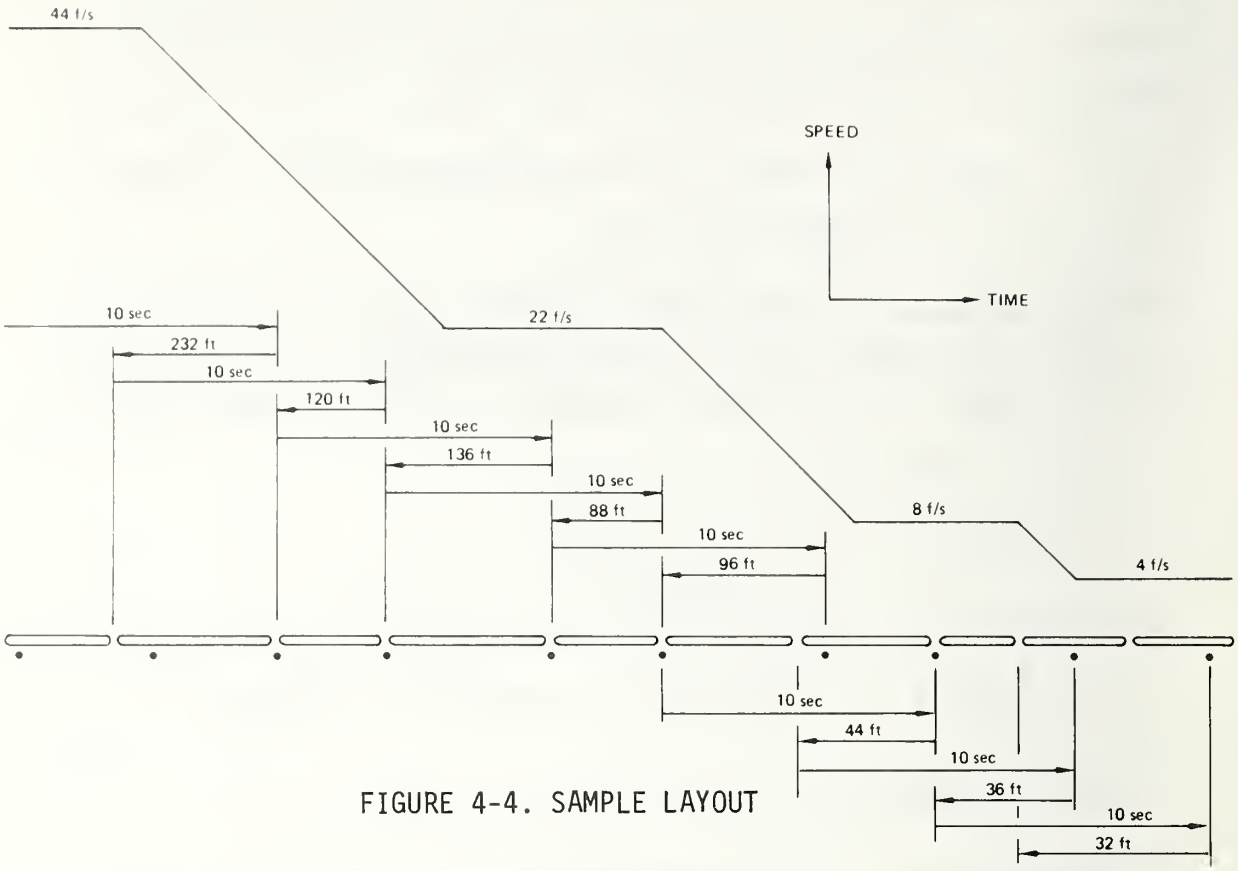


FIGURE 4-4. SAMPLE LAYOUT

For acceleration zones the layout procedure is similar to constant speed case 1 since the headway constraint is dominant. All blocks are laid out with lengths corresponding to half the minimum headway.

4.2.2.2 MPM CAS Layout Procedure. The initial layout for Phase I was provided by Bendix. A graphical technique illustrated in Figure 4-5 was used. The two outer curves each represent a time/distance plot for a vehicle traveling with a nominal speed profile accelerating and decelerating in perfect conformity to guideway speed commands. The vehicles are separated by the minimum headway (12.8 seconds for MPM). The middle curve is vertically offset from the first curve by the minimum allowable separation (vehicle length plus worst case stopping distance for the trailing vehicle). Blocks are laid out by stair stepping between the trailing vehicle (right most curve) and enforced separation (center curve). Safe tone boundaries are placed at positions corresponding to the ends of the vertical bars. PDs are placed at positions obtained by extension of the vertical bars.

In Figure 4-5 PDs are not aligned with safe tone boundaries.

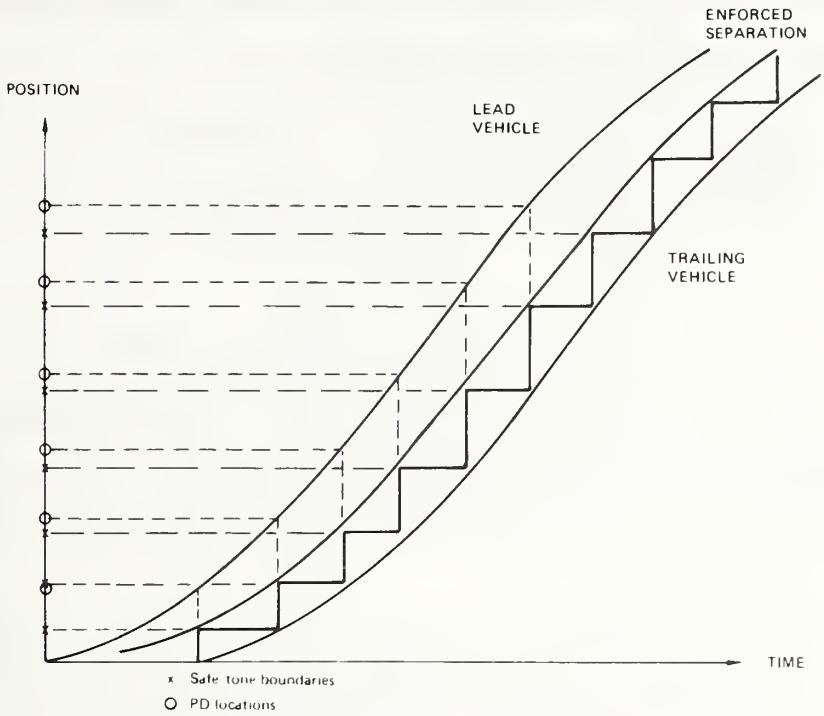


FIGURE 4-5. TIME/DISTANCE PLOT FOR CAS LAYOUT

In Figure 4-6 alignment has been achieved by trial and error process.

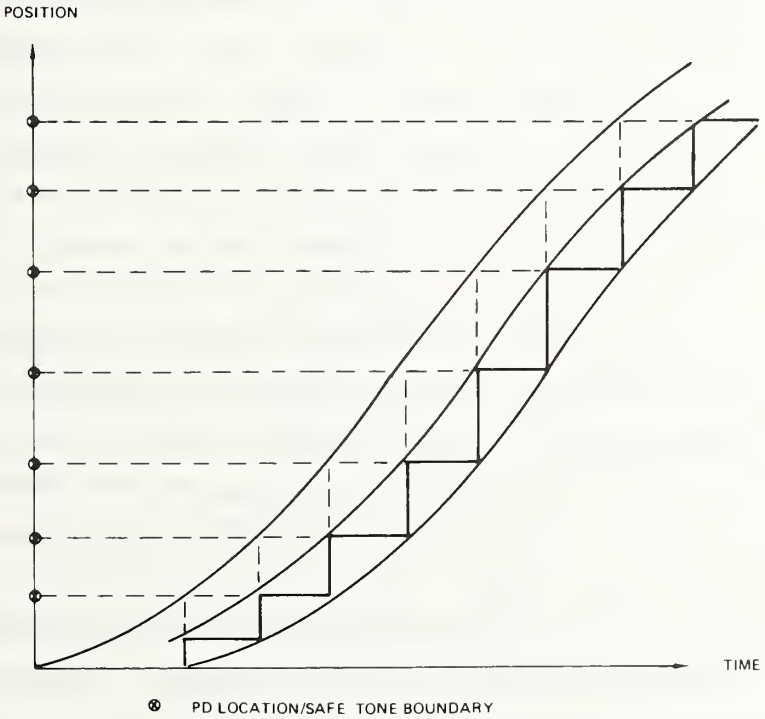


FIGURE 4-6. LAYOUT WITH BLOCK ALIGNMENT

The CAS layout provided by Bendix was evaluated by Boeing using another graphical technique illustrated in Figure 4-7 in which vehicle separation is plotted against lead vehicle position.

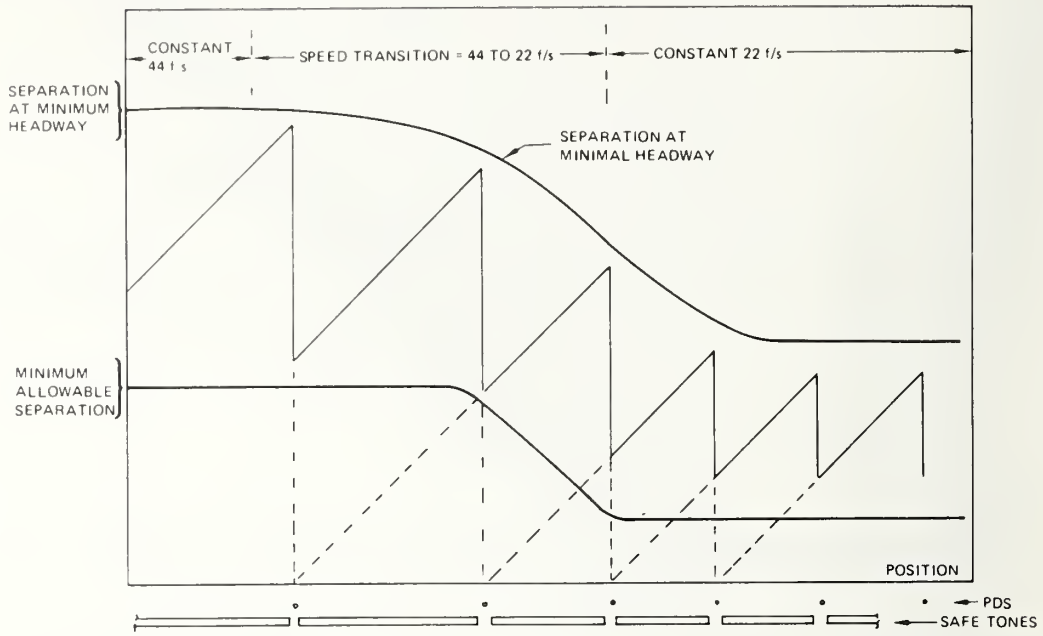


FIGURE 4-7. CAS/LAYOUT VEHICLE SEPARATION Vs. POSITION

The upper curve plots the separation between two vehicles traveling at minimum headway. This separation must not result in loss of safe tone for the trailing vehicle. The lower curve plots a separation equal to minimum separation (vehicle length plus trailing vehicle stopping distance). This separation must result in loss of safe tone for the trailing vehicle. The system is safe and operable for any layout such that the enforced separation lies between the two curves. The solid "saw tooth" curve illustrates the enforced separation resulting from an acceptable layout. The corresponding layout is included for reference. The dotted lines show the geometric relationship between the layout and the enforced separation. Note that the vertical drop for each step occurs at a PD. This results from the safe tone status change triggered each time a vehicle arrives at a PD. At that point the off status moves forward one block. Between PDs the enforced separation increases as the vehicle moves forward since the safe tone which is off does not change until the next PD is reached. The resulting slope is 45 degrees since separation and position

are plotted to the same scale. Safe tone boundaries occur at the intersection between the extended 45 degree dotted line and the position axis. The layout shown illustrates the geometry when safe tone boundaries are aligned with PD position. The MPM CAS layout adheres to this convention. Exceptions occur only where geometric constraints did not allow alignment.

Phase II CAS Layout. For Phase II standardized block lengths were used to the extent possible. On the main guideway the standard length was 5.6 seconds. This yields 123 feet for 22 ft/s guideway and 185 feet for 33 ft/s guideway. Adjustments were made for factors such as speed transitions, station control boundaries, and ramp intersections.

The initial layout began by locating the station berths (stop loops) and the channel CAS blocks. These blocks were located based on vehicle speed, grade, stopping distances, and acceptable margins. After the channel and ramp CAS blocks were defined out to the main guideway, the CAS blocks on the main guideway between stations were located, again using grade, speed, and stopping distances in determining proper block lengths.

Commensurate with the CAS layout other control elements, such as speed transitions and switch loop locations, were also defined as they too contribute to the measure of safety and operability of the system.

Upon completion of the initial layout of the CAS, computer programs were used to verify that the locations defined were viable and afforded a safe operable system. A computer program titled "MERGE" was used to verify that all merges, both channel-to-ramp and ramp-to-main guideway, were safe and operable.

The "MERGE" program simulates two vehicles being dispatched from two separate station channels and merging to the common path (rap) with an interval (separation) of 12.8 seconds. The program output was plotted, then used to verify the operability of the CAS layout in the merge areas under worst case conditions. This program was also used to verify the CAS layout for station ramp to main guideway merges.

After the station merge areas had been evaluated, a second computer program was used to verify that all CAS blocks in the initial layout were adequately sized and spaced such that trailing vehicle safety and operability margins were achieved. This was accomplished using a computer program titled "TRAJEK". This program simulates a vehicle trajectory in terms of time, distance, acceleration and speed, whether it is being dispatched from a berth or whether it is on any section of guideway, and treats that vehicle as though it were an ideally profiling vehicle (instantaneous response to vehicle commanded speed changes). The program locates a second vehicle trailing this ideal vehicle by 12.8 seconds. The program then simulates a defined trip for these two vehicles reporting safety and operability margins for each CAS block that pertains.

Ground Rules and Assumptions.

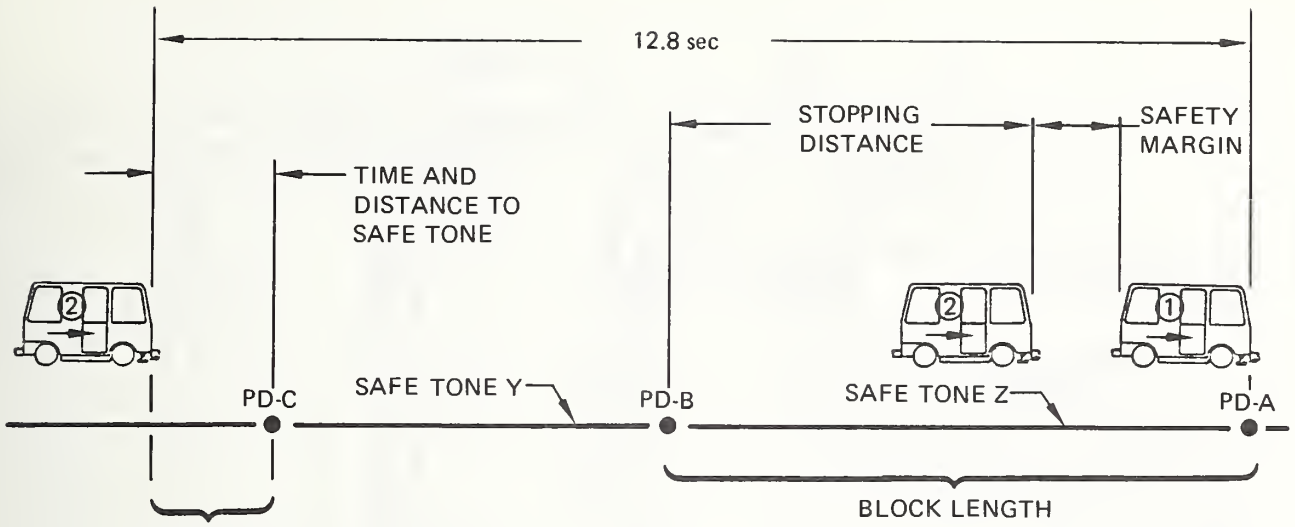
1. All CAS blocks were evaluated at 3.3 ft/s over the commanded vehicle speed.

2. Safety margins are worst case values resulting from stopping distance calculations that assumed:

   a. Vehicle 3.3 ft/s over commanded speed;
   b. Time in jerk of 1.4 seconds;
   c. Deceleration of (0.3g -10% + grade);
   d. Maximum gross weight vehicle;
   e. Delay from loss of safe tone to initiation of jerk of 0.35 seconds.

3. Operability margins are worst case values assuming the trailing vehicle is 12.8 seconds behind the lead vehicle instead of the nominal 15-second separation.

The following diagram (Figure 4-8) illustrates the relationship between block lengths, safety and operability margins.



NOTE: MINIMUM BLOCK LENGTH = STOPPING DISTANCE PLUS ONE VEHICLE LENGTH.

SAFETY EVALUATION

AS VEHICLE 1 STRIKES PD "A", SAFE TONE "Y" IS TURNED ON. IF VEHICLE 1 STOPS AT PD "A", VEHICLE 2 WILL APPLY EMERGENCY BRAKES AT PD "B.

OPERABILITY EVALUATION

WHEN VEHICLE 1 STRIKES PD "A", VEHICLE 2 WAS ASSUMED TO BE 12.8 sec BEHIND. SAFE TONE "Y" TURNS ON RESULTING IN AN OPERABILITY MARGIN (MEASURED IN TIME AND DISTANCE) BETWEEN VEHICLE 2 AND SAFE TONE "Y".

FIGURE 4-8. DEFINITION OF SAFETY AND OPERABILITY MARGINS

Interpretation of Merge Operability. At merge areas a normally-off block exists in each leg of the merge. As a vehicle approaches a merge area, it will be granted priority based on first arrival at a PD prior to the merge guard loop. For the vehicle which receives priority, the normally-off guard loop will be turned on. If a vehicle is out of position as it approaches the merge and priority has already been granted to a vehicle in the other leg, the normally-off block will remain off for the vehicle in violation, and a merge conflict will be avoided. Figure 4-9 shows an example of the channel merge guard loops for Towers Station. The table included on the diagram shows a matrix of the guard loops that function as described in the preceding paragraph.

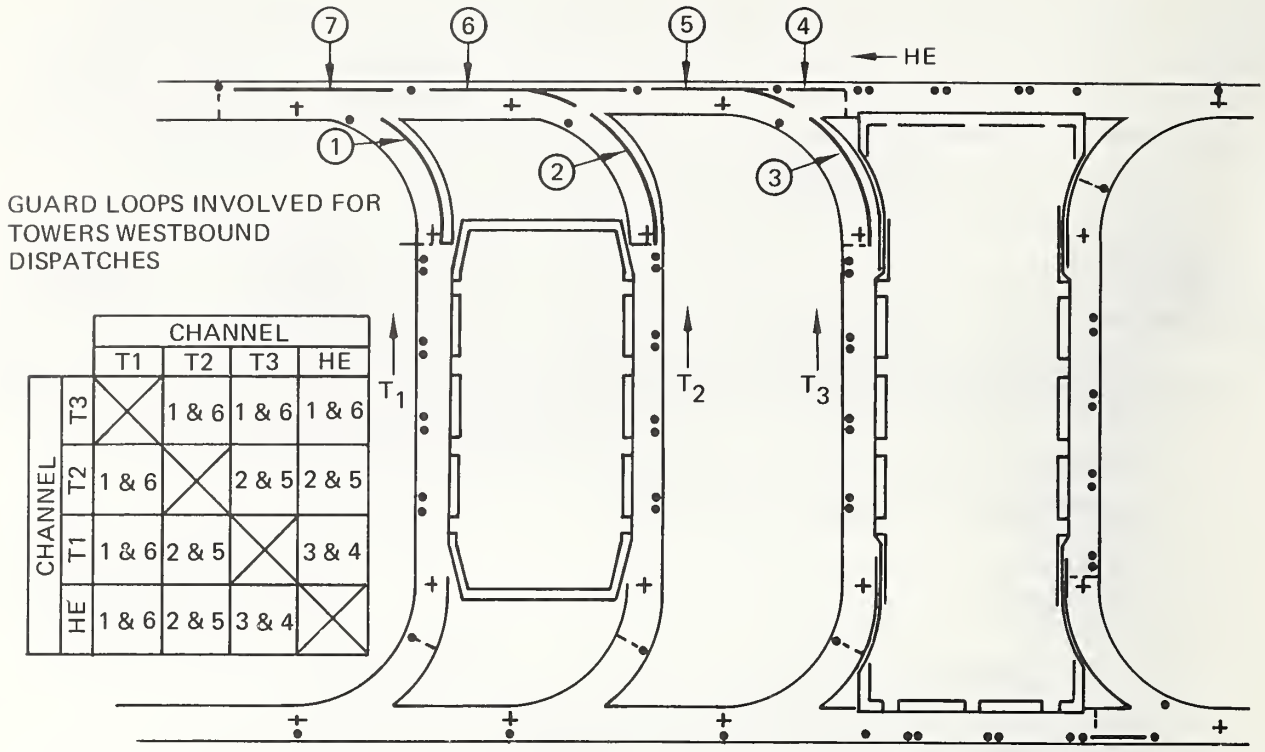


FIGURE 4-9. TOWERS STATION MERGE GUARD LOOPS

Figure 4-10 provides an example of a merge plot. The plot is shown here because it typifies the manner in whch operability and safety information for the merge guards can be obtained. The Channel T1-Channel T2 merge plot includes a four quadrant representation of the relative locations encountered by vehicles that merge at the T1-T2 (theoretical) frog after dispatch from channels T1 and T2. Each cited location is measured relative to the frog so that negative values denote relative locations encountered prior to the frog; positive values denote relative locations encountered after the frog; and the zero location denotes frog encounter. A point located in quadrant 1 denotes that the vehicles are on the common path that exists for both channels beyond the frog. This quadrant contains a collision line which represents the condition that results when the same location is encountered by two vehicles at the same instant in time. Note that the general direction of motion and, therefore, time is "up and to-the-right" although time changes are not explicit.

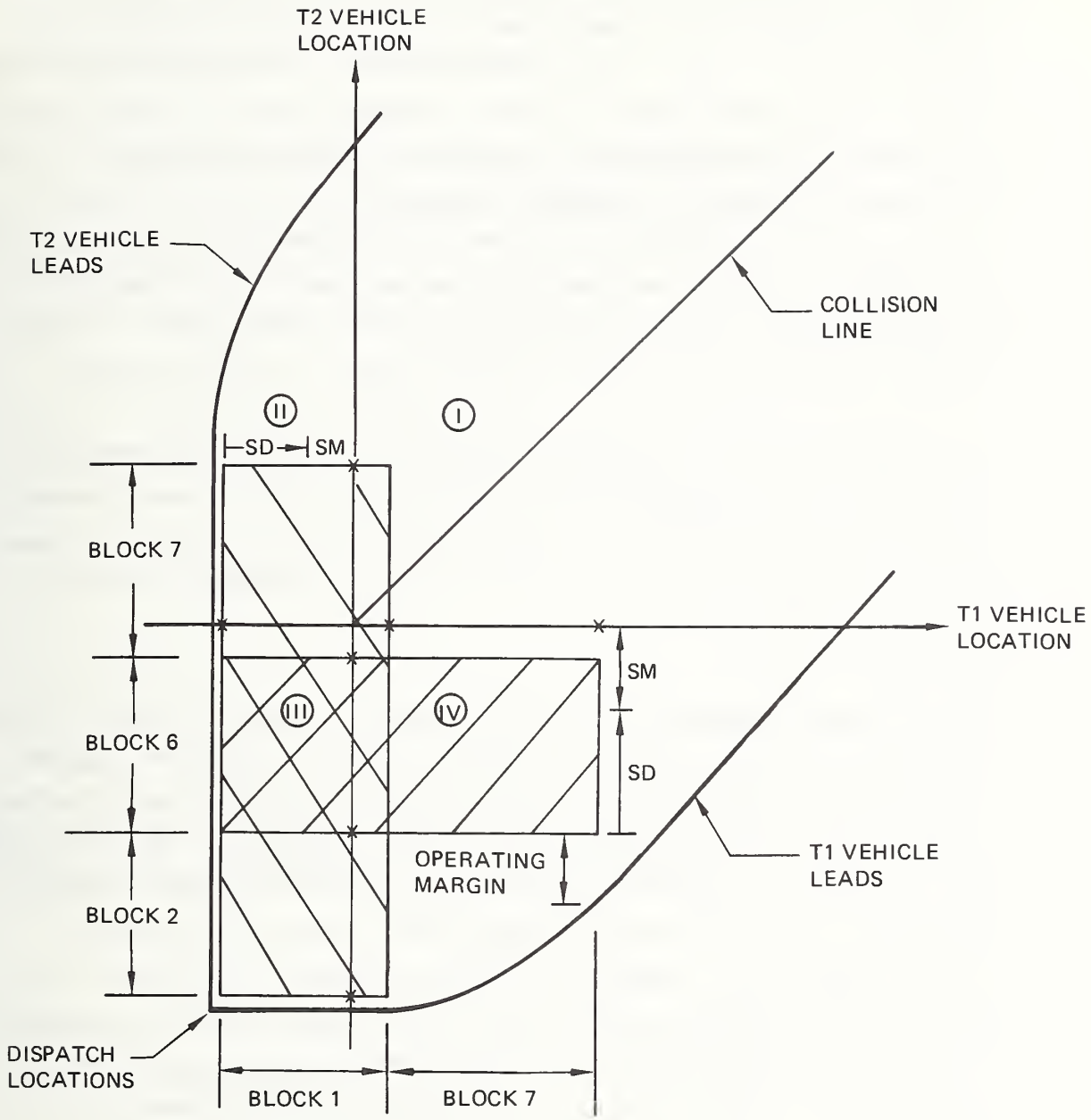


FIGURE 4-10. MERGE PLOT EXAMPLE

in location-location space. A point located in Quadrant II denotes that the T2 vehicle is located beyond the frog while the T1 vehicle is located behind the frog. A point located in Quadrant III denotes that both vehicles are located behind the frog. Quadrant IV denotes that the T1 vehicle is located beyond the frog while the T2 vehicle is located behind the frog. The line labeled "T2 Vehicle Leads" is the locus of points that results when a vehicle in channel T2 leads

a vehicle in channel T1 to and beyond the frog by 12.8 seconds. The vertical portion of that locus implies motion by the T2 while the T1 vehicle remains fixed at his dispatch location. The remaining portions of that locus exhibit motion of both vehicles, that is, neither vehicle is at rest. These portions of the locus include curvature that results from the differences in relative speed profiles at a given instant in time. The separation between vehicles (caused by the speed profiles) at a point of interest on the locus can be obtained by algebraically differencing the vehicle locations which define that point. Similar remarks pertain to the locus of points labled "T1 Vehicle Leads".

The relative locations of presence detectors along the two channel paths behind and beyond the frog are indicated by Xs. These presence detector locations define the boundaries of the CAS blocks which have been superimposed upon the plots as squares or rectangles as their placement requires.

The relationship between the vehicle location lines and the CAS blocks establish the extent of operability and safety for the merge guards. In the figure, the merge guards are labeled as blocks 1 and 6 per the scheme shown in the previous figure. The cross-hatched blocks indicate two conditions. The first condition pertains to the case in which where the T1 vehicle has established merge priority over Block 6. In this case, the T2 vehicle will apply emergency rate brakes if it enters Block 6 while T1 has priority. The second condition pertains to the case in which the T2 vehicle has established merge priority over Block 1. In this case, the T1 vehicle will apply emergency rate brakes if an anomaly occurs such that the T1 vehicle enters Block 1 while T2 has priority. The merge guard placement is operable if the previously discussed loci do not penetrate these blocks. The operability margin is measured in terms of the horizontal or vertical distance between a point on the locus and the appropriate CAS block.

The merge guard placement is safe if the distance from the start of the merge guard to the frog point exceeds the worst case stopping distance.

The safety margin is the difference between these distances. The worst case stopping distance (SD) and merge guard safety margin (SM) are shown for the merge guards in Figure 4-10.

Two safety and operability margins were determined for each merge guard. First, the margins were computed for merging vehicles as discussed above. Next, the TRAJEK program was used to determine margins for adjacent vehicles crossing the block from the same leg. In this case the available stopping distance is the block length less vehicle length.

4.2.2.3 Physical CAS Layout. The preceding discussion provides a CAS layout without regard to geometric details of vehicle design. This approach simplifies the layout effort and results in a layout which is independent of those details. Minor adjustment can then be made to allow for these details.

PD Placement. For the MPM vehicle, the physical position of each PD is shifted 2.4 feet to allow for the separation between the PD activator (magnet) and safe tone receiver (antenna). This shift is not used for the forwardmost berth PD in a channel since the berth safe tone is always on and the next safe tone is normally off. The vehicle geometry and resulting PD placement is illustrated in Figure 4-11.

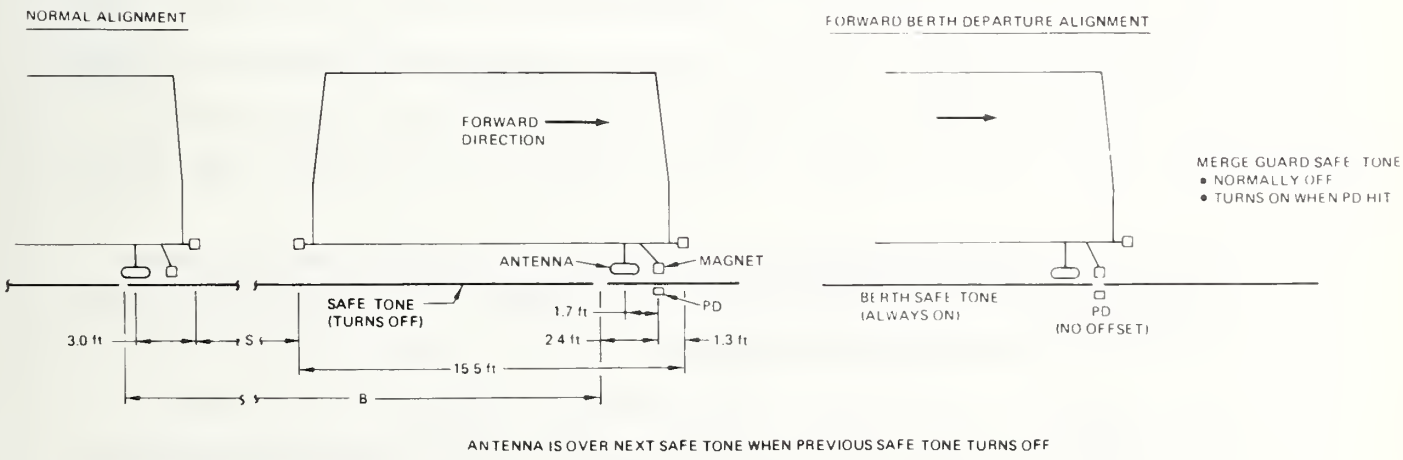
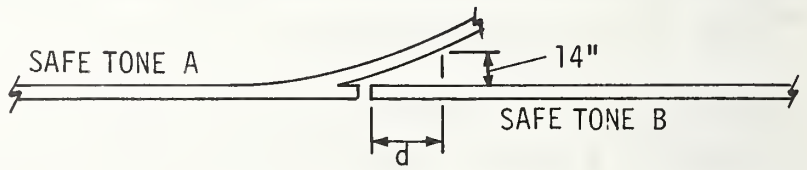


FIGURE 4-11. PD/SAFE TONE ALIGNMENT

Safe Tone Placement. Safe tone physical positions must allow for the following factors:

1. Merge guard and switch guard loops must allow for the front overhang (i.e., the offset between the front of the vehicle and the safe tone antenna).

2. A safe tone can be detected when it is not directly under the vehicle antenna. The MPM vehicle antenna can detect safetones with a 14-inch lateral offset. This can substantially reduce the effective length of certain safe tones as illustrated below.



The length of safe tone B is effectively reduced by d = distance from start of B to point at which A and B are 14 inches apart.

The above situation (referred to as safe tone coupling) is best avoided by a layout which provides a minimum lateral offset of 14 inches between adjacent safe tones. Shorter offset is acceptable but achieves nothing. In the above example the boundary between safe tones A and B could be moved by the distance d without changing the safety for safe tone B.

4.2.2.4 Disparity Zone Layout. The disparity zone layout adopted for Phase IB was established by a trade study. The following discussion is drawn from the resulting report.

The disparity zone concept evolved as a compromise between two extremes in terms of how much of the total station/guideway system should experience

loss of safe tone (resulting in emergency braking to all moving vehicles within the zone) in response to a detected disparity.

The least costly concept would define one all encompassing disparity zone, such that a CAS disparity anywhere in the system would remove all safe tones. The negative impact on system availability and the large number of occupied vehicles subjected to emergency braking are the penalties paid for this least expensive disparity zone concept. The other extreme is one CAS disparity zone for each safe tone loop. At most, one vehicle would be subjected to emergency braking with trailing vehicles commanded to stop by normal brakes. However, the cost and complexity would be unacceptable for this approach.

In seeking a compromise between these two extremes, the following factors were considered:

1. Compatibility with planned procedural responses to vehicle down anomalies other than CAS disparity.

2. Number of vehicles and their passengers subjected to emergency braking.

3. CAS reliability as a funcion of number of zones, with associated disparity detection and safetone removal hardware.

4. Fleet availability.

5. Cost.

The guideway/station layout was examined in conjunction with on-going studies of procedural responses to "vehicle down on guideway" anomalies. Key to the development of these procedures was the development of the concept of Traffic Control Segments (TCS). Each TCS is a segment of guideway which can be shut down without preventing vehicle travel through other segments.

It became apparent that the CAS disparity zones should be compatible with the TCS so that the operator/software procedures could apply to CAS failures as well as to other vehicle down anomalies.

In addition, the question of the number of vehicles which would be emergency braked to a stop with a CAS zone disparity arose, and the data presented in Figure 4-12 was generated.

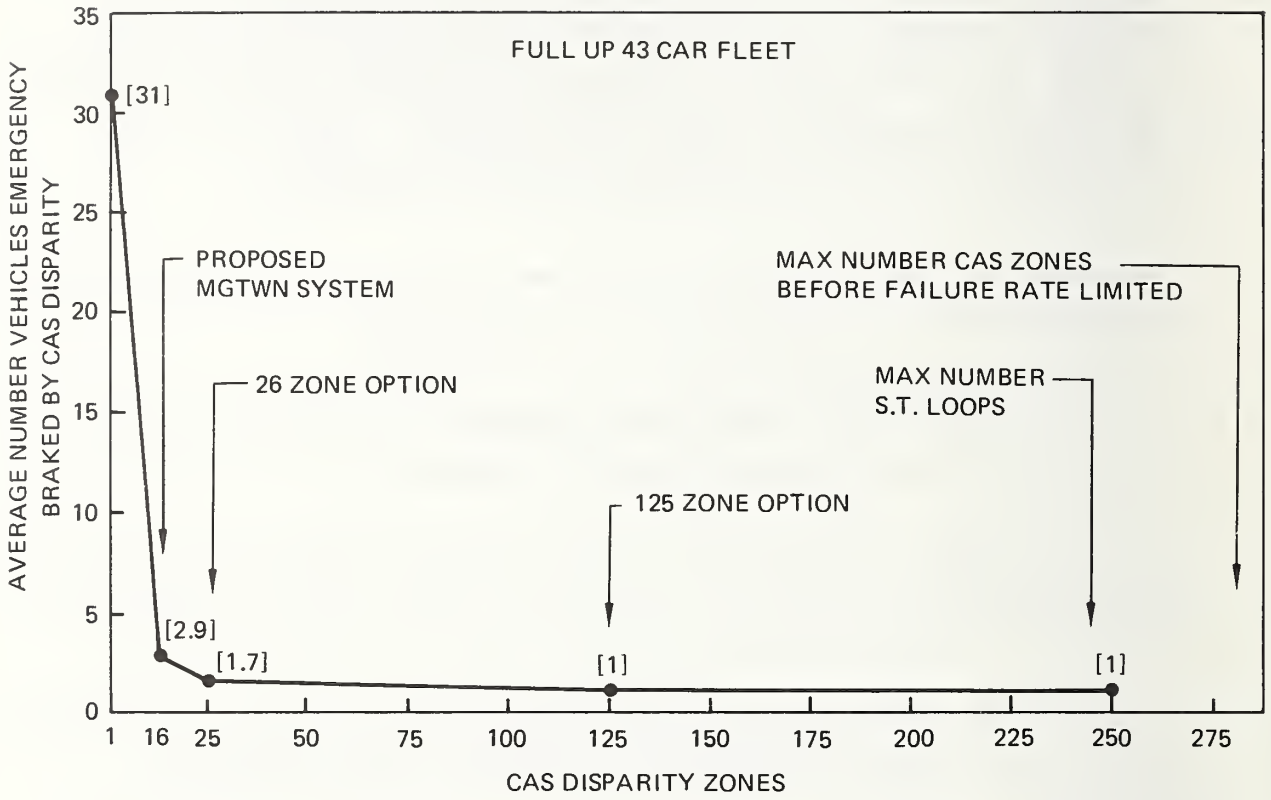


FIGURE 4-12. VEHICLES EMERGENCY BRAKED VS. NUMBER CAS DISPARITY ZONES

The knee of the "emergency braked vehicles" curve is clearly somewhere between 10 and 25 zones. Subsequent analyses indicated that 16 zones on the Morgantown track layout, (13 on the main guideway, two in Beechurst, and one in Maintenance), (a) would be compatible with TCS, and (b) would subject an average of 2.9 passenger carrying vehicles (and not more than a maximum of 4) to emergency braking in response to a single CAS zone disparity. The maximum number of vehicles that could be subjected to emergency braking in each CAS zone (for Phase IB in which every third null is empty) is summarized in Table 4-2.

TABLE 4-2. MAXIMUM NUMBER OF VEHICLES EMERGENCY BRAKED BY DISPARITY

CAS ZONE	PHASE IB MAX. NO. VEHICLES EMERGENCY BRAKED
C1	3
C2	3
C3	3
C4	2
C5	3
C6	3
C7	2
C8	3
C9	3
C10	4
C11	2
C12	4
C13	4
CBS (Beechurst South 8 ft/s)	2
CBN (Beechurst North 8 ft/s)	2
CM (Maintenance 8 ft/s)	6*

*No Passengers

Next, a CAS zone concept which would subject a maximum of one vehicle to emergency braking was considered. Since vehicles are normally separated by more than two CAS loops, a two loops-per-CAS-zone concept was costed. It was determined that approximately 125 zones would be required. Finally, a zone concept which would subject an average of 1.7 (max. 2) vehicles to emergency braking was examined. This resulted in 26 zones. Trade data, and assumptions used in the studies are presented in Table 4-3.

The differences between 16 and 26 CAS zones in terms of system downtime is approximately 22 minutes per year; in terms of number of passengers subjected to emergency braking, the difference is estimated at 227 passengers per year.

TABLE 4-3. CAS ZONE TRADE DATA

1. DOWNTIME

(a) Downtime per emergency braked (EB) vehicle is 0.5 minute.

(b) 36.5 disp./year are expected (CAS MTBF = 240 hours)

36.5 disp. x 0.5 min./disp. = 18.25 min/year/veh.

Zones	Avg. # Veh. EB	Downtime/Veh./Year	Downtime/Year
16	2.9	18.25 min.	52.93 min.
26	1.7	18.25 min.	31.03 min.

2. PASSENGERS SUBJECTED TO EMERGENCY BRAKING

(a) 9.316 psng./veh. in 11/24 day schedule mode

(b) 1.7 psng./veh. in 13/24 day demand mode

(9.316 X 11/24) + (1.7 X 13/24) = 5.188 average psng./veh.

(c) Same average number vehicles moving in both modes.

Zones	Veh.EB Avg. #	Psng./Veh. Avg. #	Disp./Year	Psng. EB #/Year
16	2.9	5.188	36.5	549
26	1.7	5.188	36.5	322

The reliability impact of the additional disparity detection hardware associated with added CAS zones proved to be negligible. Allotted failure rate would not be reached by adding up to 250 CAS zones (i.e., one for each loop).

In summary, increasing the number of CAS zones over the 16-zone concept would accrue significant cost while providing:

1. No improvement in compatibility with traffic control procedures for recovery of the fleet from non-normal to normal state as a result of a detected CAS disparity;

2. At best a trivial improvement in system availability; and

3. Little significant reduction in the number of passengers subjected to emergency braking as a result of a detected CAS disparity.

For these reasons the 16-zone CAS concept was selected as most cost effective for Phase IB.

Phase II. The CAS zone layout adopted for Phase IB proved to be very successful. As a result, the same layout concept was applied to Phase II. That is, one zone was used for each Traffic Control Segment for a total of 29 zones. The only problems encountered involved the exact choice of boundaries. It is important to place the boundaries carefully so that a disparity in one TCS will not unnecessarily block entry to another TCS. In Phase II an early design review detected one such error which was corrected.

4.2.3 CAS Reset Capability

A reset capability is required to initialize the CAS at start up and after CAS failures, such as false and missed PDs. The original design provided only capability to clear all blocks in a station. It was quickly found that some means was required to set individual blocks occupied. This was accomplished in Phase IB by addition of a Test and Maintenance (T&M) Panel which allows maintenance personnel to modify block occupancy by manually generating PD hits.

The test panel is required to perform the following functions:

1. Generate simulated PD hits.

2. Generate simulated switch verification signals.

3. Indicate which safe tones are on.

The panel is laid out on a diagram of the guideway controlled by the station. (See Figure 4-13.)

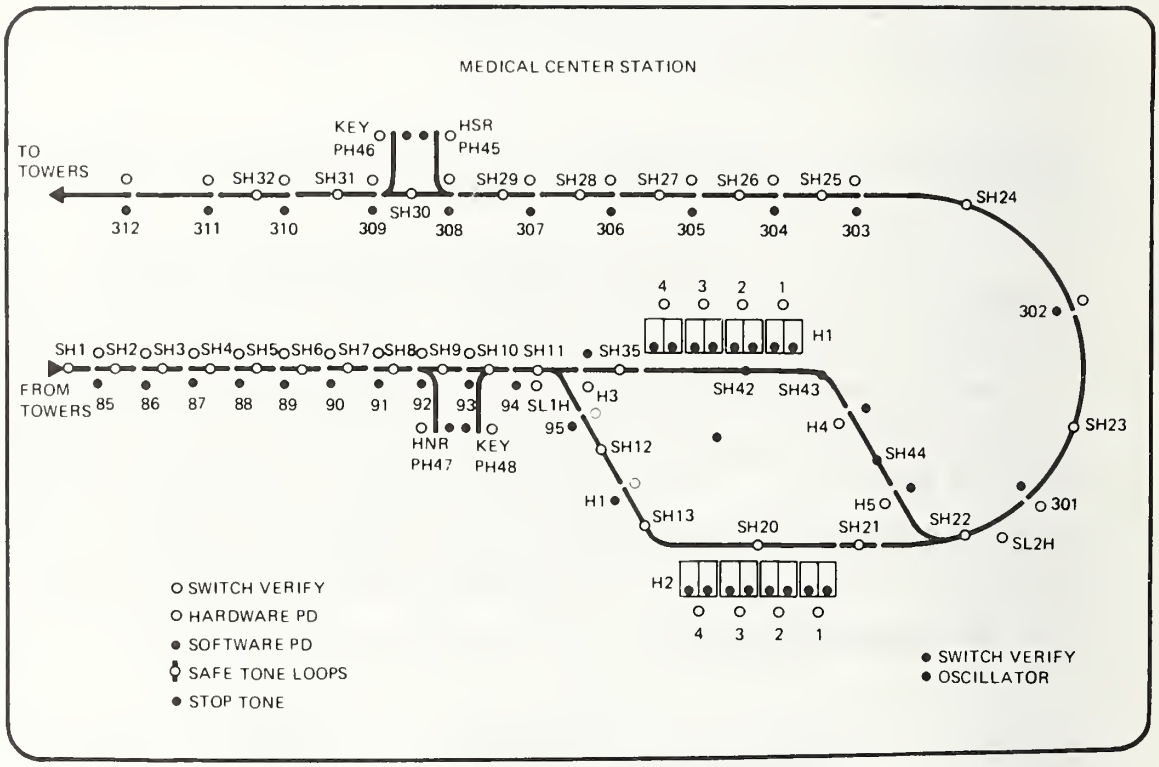


FIGURE 4-13. TYPICAL T&M PANEL

A push button is installed for each PD (hardware and software) and for each switch loop. A light-emitting diode (LED) is installed for each safe tone. Each PD push button is a normally open switch connected across the corresponding PD wires.

Pushing a PD button has the same effect on the CAS as an actual vehicle "hit." Similarily, pushing a switch loop button will apply a 22 kHz signal, modulated at 50 Hz, to the corresponding switch verification receiver input.

An LED is connected, with a series resistor across each safe tone loop, so that it lights when its respective safe tone is on. The test panel is used for the following:

1. Periodic verification of CAS integrity. With all parts of the CAS operating normally, any scenario of vehicle motion can be simulated (e.g. merge conflicts, switch failure, headway violation), and the response of the CAS in controlling safe tones observed. If this response is correct for all scenarios, it can be assumed that the CAS, with the possible exception of the fail-safe disparity detectors, has no faults in it. The latter can be tested by creating intentional disparities (by pushing those buttons associated only with the computer CAS) and observing that a zone is shut down.

2. Diagnosis and isolation of faults. When a fault occurs, the test panel can be used to exercise any part of the CAS, and, thus, to determine whether the fault lies in the hardware, or in the computer, and in which loop.

3. Restart. PD push buttons can be used to establish a block occupancy state corresponding to the actual vehicle configuration.

Capability has also been provided to clear the hardware switch latch but not the software switch latch. This creates a minor operational handicap that can be avoided by activating one of the clear PDs for the switch latch.

Additional reset capability is provided for the software CAS. Reset commands are initiated by the central operator. The original design provided the following reset capabilities:

1. Zone clear - clear all blocks in a disparity zone;

2. Reset Block - set or clear a specific block;

3. Reset Priority Latch - set or clear a specific priority latch.

CAS reset proved to be time consuming and error prone following computer shutdown and restart with large numbers of vehicles outside station berthing areas. Therefore, an automatic reset capability was added during Phase IB. The automatic reset sets block occupancy on the basis of vehicle position data (last PD hit) contained in the operational software data base. The vehicle position data is periodically saved on a disk and is loaded whenever the computer is reloaded following shutdown. The operator has the ability to update vehicle location data and does so, if necessary, before initiating an automatic CAS reset. The software has ability to read back the last safe tone status output by the computer. This capability is used to compare the reset safe tone status to the last safe tone status output.

The following procedure is used to reset the software CAS following a computer shutdown and restart.

1. Vehicle positions are established using data previously saved on the disk.

2. The operator requests automatic CAS reset.

3. The software sets block occupancy on the basis of vehicle position data, computes resulting safe tone status, and compares that status to the last status output before shutdown. Discrepancies (if any) are reported to the operator.

4. If any discrepancies are reported, the operator adjusts vehicle location data and repeats Step 2. This procedure continues until all discrepancies have been eliminated.

5. Once satisfied that the software CAS has been correctly reset, the operator "Activates I-O" which initiates normal operation (i.e., enables output of safe tone status).

The above procedure is used only when no disparity is present. If a disparity is present (indicating that a vehicle moved while the computer was shutdown) additional action is required to clear the disparity.

The CAS disparity equipment includes a disparity latch. Whenever a disparity occurs (i.e., hardware and software safe tone status differ for more than 500 milliseconds) the 50 hertz tracer is removed for all safe tones in the zone containing the disparity. The tracer will not be restored until the disparity is cleared by inserting a "disparity override plug" into the disparity equipment for the zone. (See Figure 4-14.) The override plug restores the 50-hertz tracer and resets the disparity latch.

When a disparity occurs, maintenance personnel are sent to the station involved. The cause of the failure is determined and corrective action is taken. If the disparity was caused by a missed PD (hardware or software) the PD is activated on the T&M panel. The override plug is then inserted and removed to clear the disparity latch.

If the disparity was caused by a false activation of a software PD, vehicle location data is corrected (if necessary) and automatic CAS reset is performed. False activation of a hardware PD requires more involved action due to the inability to clear an individual block. Usually PDs ahead of the falsely activated PD can be sequentially activated until all blocks in the sequence have been cleared. Under some conditions it is necessary to insert the disparity override plug and clear the affected guideway section by advancing the vehicles. (When an override plug is inserted, operating procedures allow movement of only one vehicle at a time. This is because only single thread CAS protection is available with the plug inserted.) The plug is then removed before normal operation is restored.

A special, single zone, reset capability is provided for the Maintenance area test track. This is because the test procedure used to test vehicle response to loss of safe tone creates disparities. The single zone reset is incorporated as a partial station automatic reset in the software and a single zone reset in the hardware CAS at Maintenance. The current reset capability of the software CAS consists of:

1. Station reset,

2. Partial station reset,

3. Priority latch reset,

4. Block reset.

The first two capabilities involve automatic reset as previously described. The last two are identical to those originally provided.

4.3 DESIGN IMPLEMENTATION

The collision avoidance system is divided into four functional areas: vehicle detection, CAS logic, disparity detection (and reaction), and safe tone control. Vehicles are detected by a system of presence detectors discussed in the following section. CAS logic is provided by redundant hardware and software systems. The hardware CAS logic is hardwired in the older stations and provided by microprocessors (firmware CAS) in the newer stations. The firmware and software CAS design differ completely to avoid common mode failures. The hardwired, software, and firmware CAS logic are discussed in three following sections. Two additinoal sections describe the disparity equipment and the safe tone subsystem.

4.3.1 Presence Detectors

The presence detector sensors consist of dual quad redundant reed switches. The reed switches implemented in Phase IB replace magnetometers which were initially used (with poor results) in Phase IA. The following discussion references Figure 4-14.

Each card contains the electronics for four presence detector (PD) locations. Its purpose is to convertthe reed switch closure of the presence detector guideway element into high level logic signals with a high degree of noise immunity. Each PD location has two independent contact pairs, the A pair and the B pair, both of which are normally open.

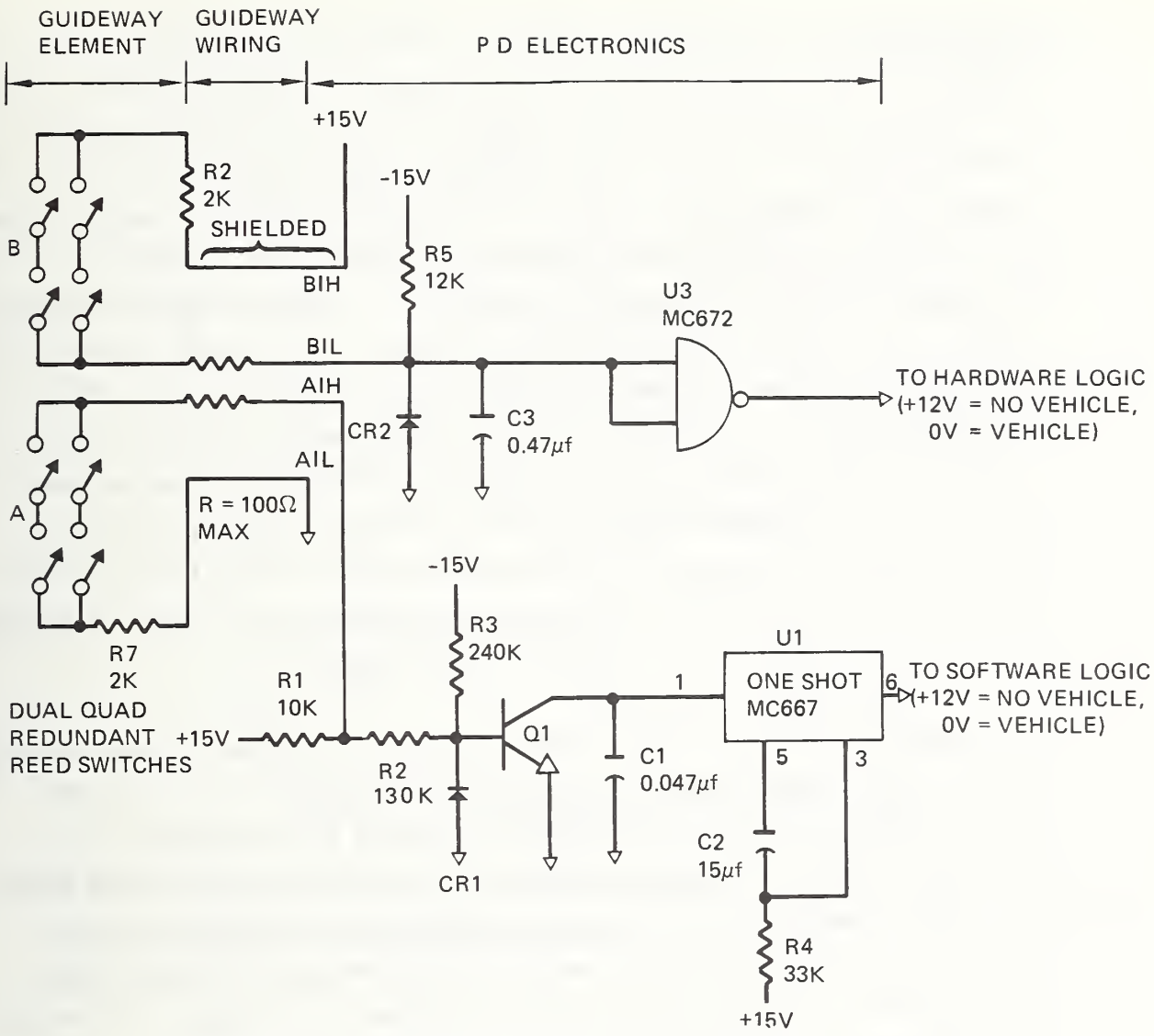


FIGURE 4-14. PRESENCE DETECTOR ELECTRONICS

This discussion will be limited to only one set of circuits on the PD electronics card since the other sets are identical. The A PD pair connects to the A1H and A1L terminals of the card. The A1L terminal is grounded to circuit ground within the card. The A1H terminal is normally held at +15 volts by pull up resistor R1. This puts a forward bias on the transistor Q1 base-to-emitter junction, turning the transistor on. The collector of Q1 will be near zero volts. The one shot, U1, will be off; its output will be about +13 volts.

When a vehicle passes the PD guideway elements, the magnet on the vehicle will cause the reed switch A contacts to close. (The contacts are

protected from high current surges by a 2000 ohm resistor in the guideway element.) Thus, a 2K-ohm connection to ground will appear between terminals A1H and A1L of the PD electronics board. This will drop the voltage of A1H to about 1.7 volts. This voltage is insufficient to hold the forward bias on the base of Q1, and Q1 ceases to conduct. The collector voltage of Q1 will rise toward +15 volts as the current supplied by the input circuit of U1 charges capacitor C1. When the input voltage of U1 reaches about +8 volts, U1 will trigger. U1's output switches to about +1 volt and will maintain this output level for about 300 ms at which time its output will return to its high level regardless of what its input level is. This period is sufficient to ensure that the PD will be sampled at least twice by the data acquisition unit of the station's electronics. The charging time of capacitor C1 gives this circuit considerable noise immunity and makes the circuit insensitive to input pulse durations of less than about 1/2 ms.

Simultaneously with the A pair switch closure, the B pair closes placing a 2K-ohm connection between input pins B1H and B1L. This raises B1L voltage level, which had been clamped to ground by the diode CR2, to about +11 volts. The capacitor C3 must be charged in the process making the circuit immune to short duration noise spikes (C3 charge time is about 1 ms). When the voltage across C3 reaches about +8 volts, the nand gate U3-C will have logic "1" on its input; its output will switch from +13 volts to about +1 volt.
It will maintain this signal level until the PD contacts open and the signal level across C3 drops below +8 volts. Resistor R5 provides the current sinking source for discharging capacitor C3 and pulling down U3's input to the clamping level of diode CR2 when the B pair opens. The output pulse width is about 10 ms.

4.3.2 Hardware CAS

The following discussion references Figure 4-15 which is a schematic of the hardware CAS logic used in the Beechurst and Walnut stations.

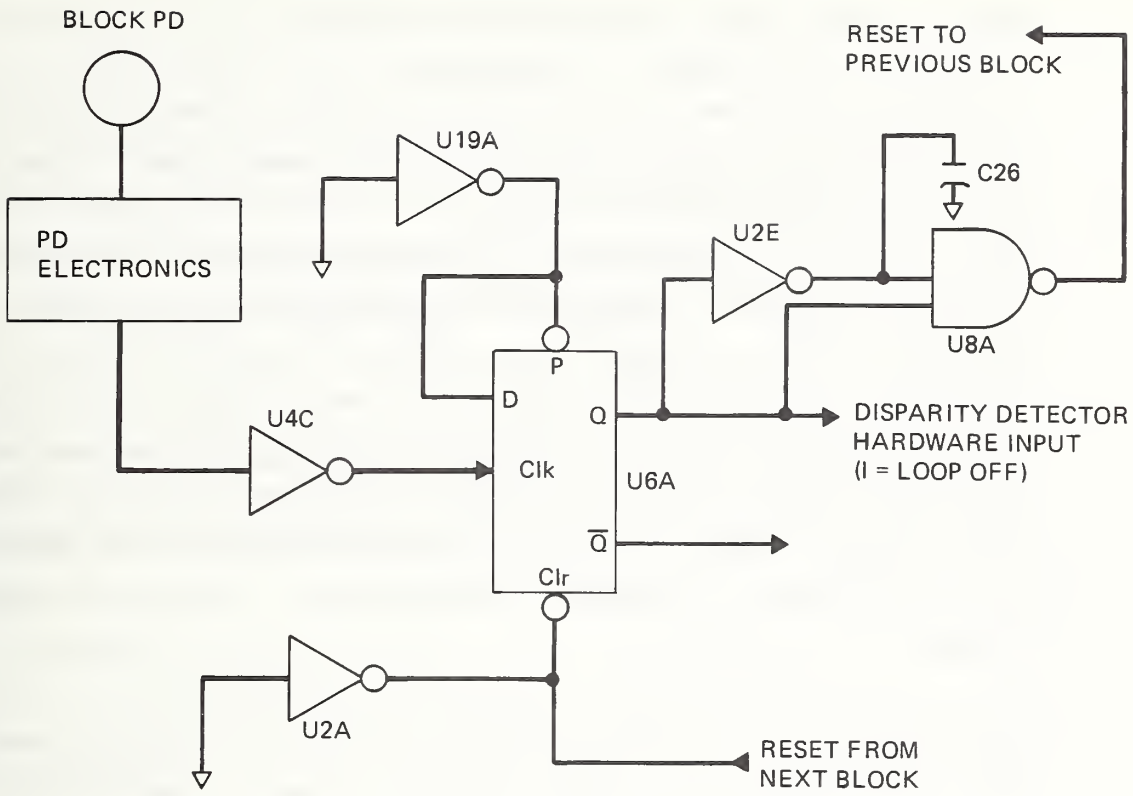


FIGURE 4-15. HARDWARE BLOCK OCCUPANCY LOGIC

A microprocessor performs the hardware logic functions in Medical Center, Towers, Engineering, and Maintenance stations. Only the discrete hardware logic will be described here.

The presence detector's input quiescent state is approximately +13 volts. When a vehicle is detected this signal level will drop to approximately +1 volt. The duration of this +1-volt level is dependent primarily on the speed of the vehicle's passage over the detector.

This signal from the PD electronics is the input to U4C which converts the high level input signal to a TTL compatible signal level and inverts the sense of the signal (i.e., a high level input gives low level output, and the converse). When the input level drops below 8 volts, the output level will rise. The positive rising edge of this signal will trigger the type-D flip-flop U6A. The D input of this flip-flop is held high by the output of the hex inverter U19A whose input is grounded. The trigger action will set the D flip-flop Q output to the low state (logic 0) and the Q output to the high state (logic 1). The Q output (now

logic 1) is the input to the disparity detector. The hardware input to the disparity detector is inverse safe tone status, hence, a logic 1 indicates safe tone off. The action of the Q output going high triggers the pulse forming circuit U2E, U8A, and C26. When Q goes high, both inputs of U8A are momentarily high since capacitor C26 holds the inverted input high until it discharges below the U8A threshold. The output of U8A is, therefore, a negatively going pulse which is an input to the previous block occupancy logic circuit. The action of this reset pulse can be seen by applying it to this same circuit. Notice that the flip-flop clear input is held high by U2A which is wired-or with nand gate of the pulse forming circuit. The negatively going pulse pulls the clear input low, which resets the flip-flop, and therefore the safe tone loop is turned off as Q goes high. This is the reset action.

Merge Protection. The merge protection logic is also part of the hardware CAS. The schematic for a typical merge is shown in Figure 4-16.

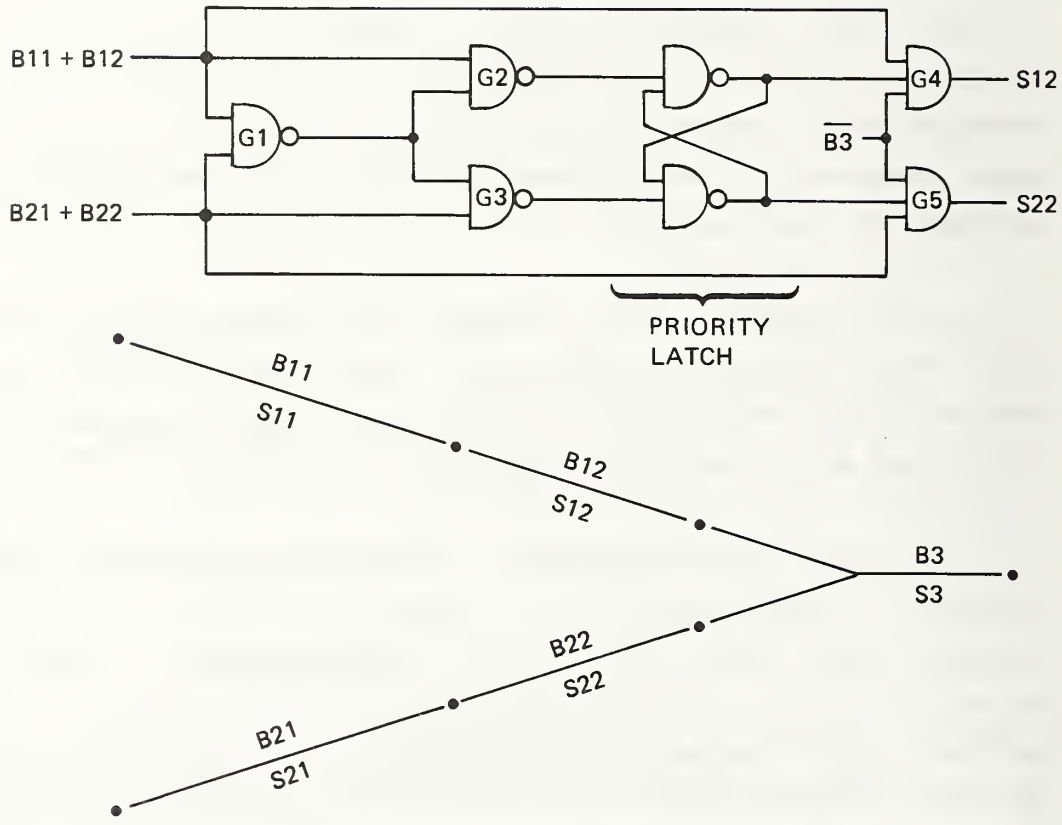


FIGURE 4-16. MERGE PROTECTION LOGIC

A vehicle approaching a merge via either leg will encounter a guard loop, S12 or S22, which is normally off. These loops are normally off since both B11 + B12 and B21 + B22 are low, and therefore, the outputs of gates G4 and G5 are low. If a vehicle is not detected when approaching a merge, it will be stopped since the guard loops are normally off. When a vehicle enters one leg, for example B11, then B11 + B12 is high while B21 + B22 remains low (assuming all other blocks are unoccupied). The output of gate G1 is high; the output of gate G2 is low; the output of gate G3 is high. The output of the priority latch which feeds gate G4 is, therefore, high. Since all inputs to gate G4 are high, the output is high and safe tone S12 is on. Safe tone S22 is off since both B21 and B22 are low as is the priority latch output to gate G5. If this vehicle continues through the merge without the entrance of a second vehicle into the opposite leg, the S12 guard loop is turned off behind it (since B11 + B12 goes low and, therefore, G4 goes low), and the priority latch remains in its present state (G4 input high).

Now consider the entry of a second vehicle into the opposite leg, B21, while the first vehicle is still present. The output of gate G1 goes low since both inputs are high. The output of gate G3 remains high since the B21 + B22 input is high and the gate G1 input is low. The priority latch does not change state since the gate G3 input is still high (the change of the gate of the G2 output does not affect the state of the priority latch). Safe tone S22 remains off.

Note that when two vehicles arrive simultaneously, only one safe tone is turned on since the priority latch has complementary outputs. Priority is given to the vehicle traveling on the leg through which the most recent previous vehicle passed.

A summary of the merge protection logic follows. A vehicle approaching a merge via either leg will be approaching a guard loop which is normally off. If the guard loop is not turned on, the vehicle will be stopped before reaching the merging guideway. To turn the guard loop on, several conditions must be met.

1. A vehicle must be detected in the "entrance" to a merge area (e.g., B11 in Figure 4-16).

2. The exit and opposite leg blocks are unoccupied (e.g., B21, B22, and B3 in Figure 4-16).

Immediately after a vehicle has left the block containing a guard loop, the loop is turned off and left off until turn-on conditions are again met.

Logic, in the form of a priority latch, ensures that if two vehicles approach a merge simultaneously, one will be stopped and the other permitted to proceed. The conditions are:

1. First vehicle to arrive and be detected at an entrance PD is given priority and permitted to pass - i.e., its guard loop is turned on (if the other necessary conditions, specified above, are met).

2. If the vehicles actually arrive simultaneously, and the first vehicle cannot be determined, the priority latch gives priority to the vehicle traveling on the leg through which the most recent previous vehicle passed. The other vehicle is stopped by its guard loop.

Thus, when two vehicles approach a merge, one is permitted to pass (providing downstream occupancy conditions are met), and the other is stopped.

Merge protection logic is accomplished redundantly in the software logic and in the hardware logic.

Switch Protection. Switch protection is also part of the hardware CAS. Switch protection, via switch verification logic, is incorporated into the CAS block control logic to prevent a vehicle from proceding beyond

a switch zone unless it has confirmed switching. A vehicle that does not properly verify is protected by a normally-off CAS "guard" loop at the downstream end of the switch zone. This loop is turned on only when the latched switch verification signal is present and the proper downstream headway clearance is provided. While a single fail-safe receiver is used, redundant logic paths are provided to process the receiver output.

Switch verify integration logic circuitry for both hardware and software are contained on the same circuit card but with separate integrated circuit chips for hardware and software functions. A circuit description follows.

The following analysis references Figure 4-17.

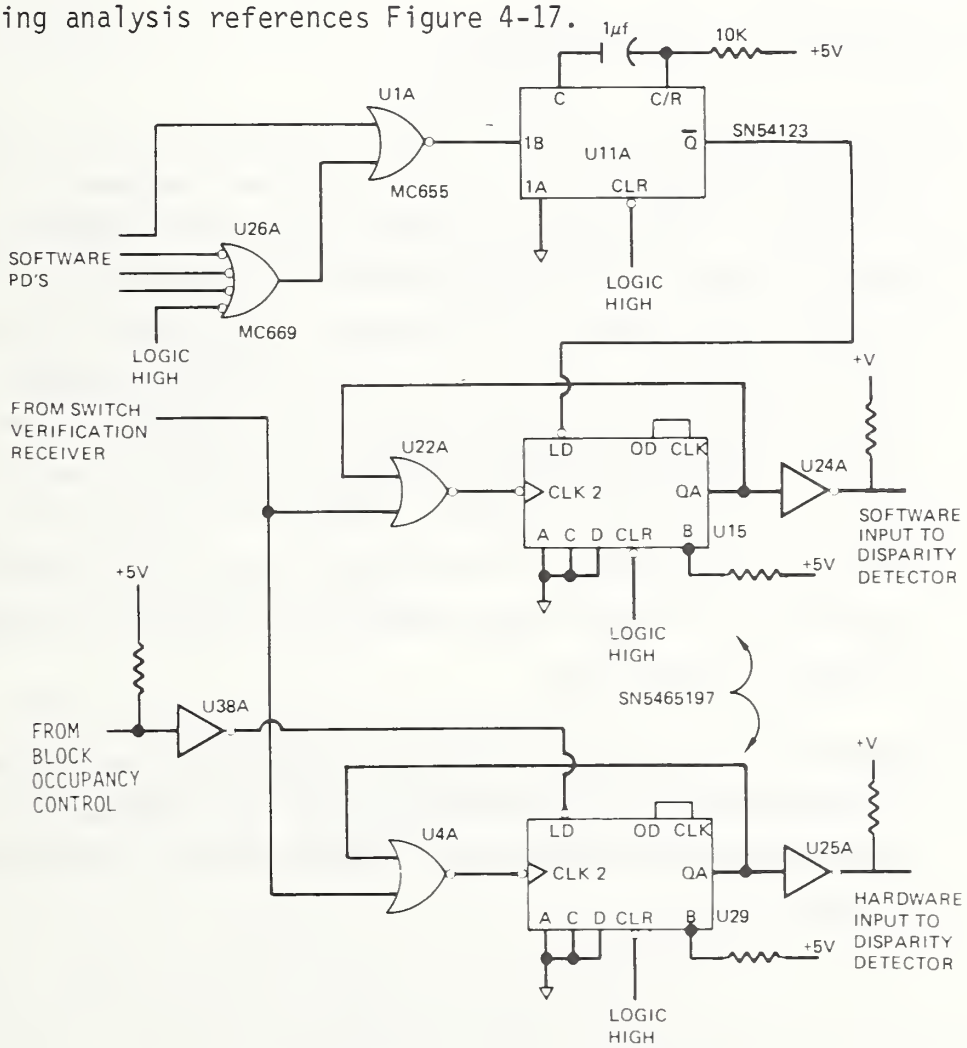


FIGURE 4-17. SWITCH VERIFICATION LOGIC

When a vehicle enters a switch verification zone, a negative software PD pulse is received by level converter U1A or U26A where it is converted to a TTL compatible signal. This positive pulse is then converted by U11A to a negative pulse approximately 3 μs wide which presets counter U15. At the same time a low switch latch control signal from block occupancy control is transmitted to the input of U38A which presets counter U29. Presetting counters U15 and U29 enables them to count the 50 or 70 Hz square wave switch verify signal received by U7A. The counters count seven pulses of the switch verify signal and output a high which is fed back into U22A and U4A to inhibit the counters from further counting until another reset signal is received. The outputs of the counters are inverted by U24A and U25A and constitute a switch verification.

4.3.3 Software CAS

Direct control of safe tone status is provided by the software CAS. The term "software CAS" is used to designate components in CAS leg controlled by software. The components include presence sensors, presence detector logic, interfacing equipment, and software. The software operates within dual string computers. The computers and the Special Purpose Equipment (SPE) are not considered CAS equipment because they serve multiple purpose control functions. The SPE transmits PD, SwitchLatch, and disparity status to both computers. Safetone status is accepted from a single (prime) computer. Control is automatically switched from the prime computer to the backup if the prime computer fails. Switchover will occur within 500 ms of failure (i.e., within the tolerance allowed for disparities).

Figure 4-18 provides an equipment diagram for the software CAS. Flow of information to and from the software CAS is shown by solid lines interconnecting the equipment. Flow of related information is shown by dashed lines.

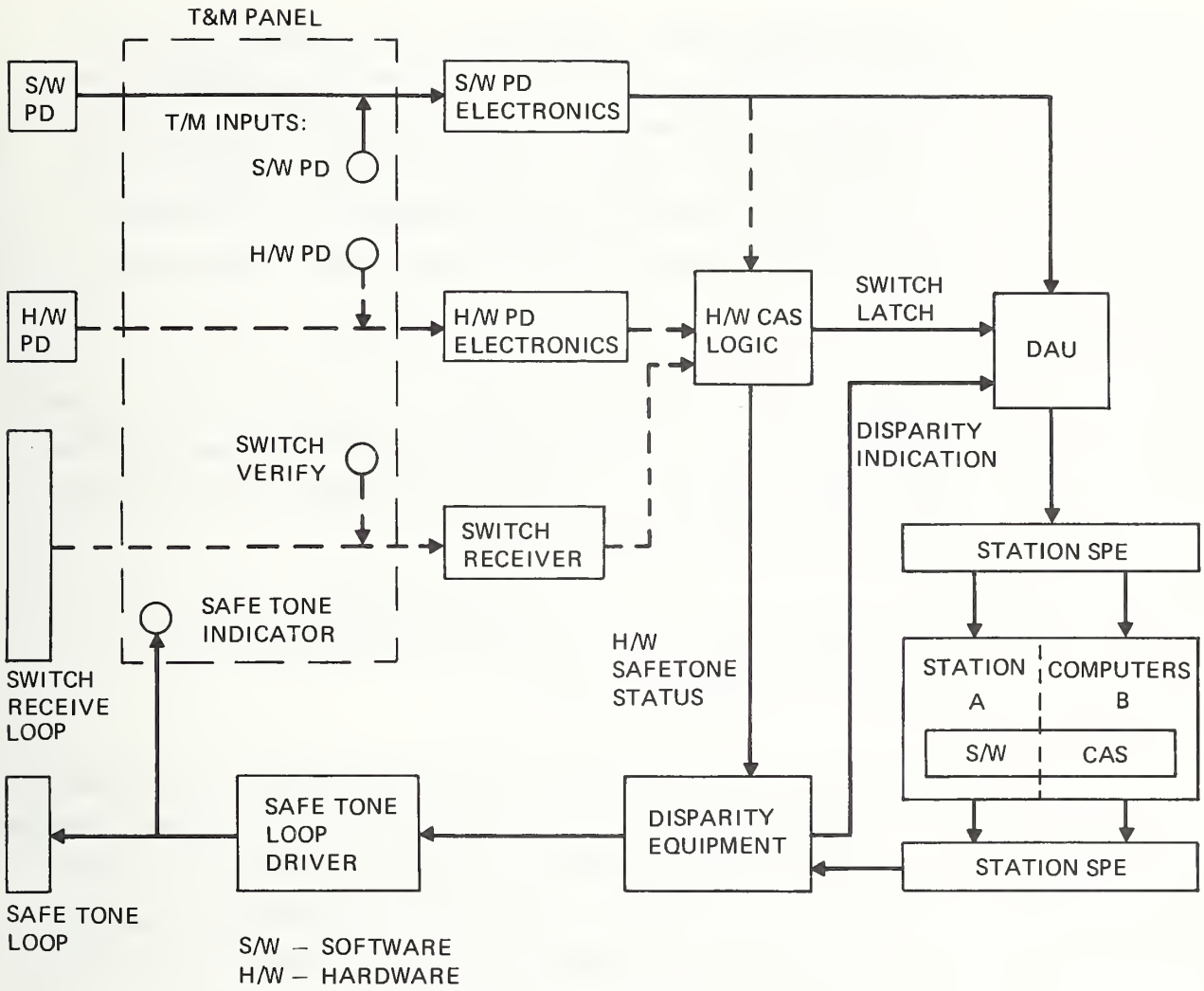


FIGURE 4-18. SOFTWARE EQUIPMENT DIAGRAM

The software CAS operates as follows:

1. When a vehicle arrives at a PD, the vehicle presence is detected by the closure of the quad-redundant reed relays which consitute the software PD. The PD activation is recorded by the PD electronics which maintains an "ON" status for 375 ms.

2. PD status is monitored by a Data Acquisition Unit (DAU). In each station, a single DAU monitors the status of all PDs. The DAU also monitors switch latch status and disparity indications.

3. Switch latch status is provided by the hardware CAS logic. The software switch latch is turned on (without regard to block occupancy) whenever switch verification is received. The switch latch remains on until the vehicle departs the switch guard or another vehicle arrives (i.e., until one of the switch latch clear PDs is activated. (See Section 4.2.1.3.)

4. The DAU reports PD, switch latch, and disparity status eight times per second. This data is transmitted to dual station computers. Except for the SPE, all computer interfaces are standard off-the-shelf equipment.

5. Data from the DAU is processed by the software CAS. The following procedure is used:

   a. PD hits are detected. A "hit" occurs when a previously inactive (off) PD is activated (turns on). Block occupancy status is updated for any blocks affected by PD hits. This is done on the basis of block occupancy equations in the CAS data base. As noted in Section 4.2.1.1, block clear expressions are evaluated before blocks are set occupied per the block set expressions.

   b. Switch latch status is updated to reflect values received from the DAU.

   c. Priority latch status is updated as dictated by block occupancy changes.

   d. Safe tone status is updated as dictated by priority latch, switch latch, and block occupancy changes. The status of a safe tone is computed if any element in the safe tone equation has changed state. Safe tone status is updated using one of five subroutines indexed by the safe tone type.

SAFE TONE TYPE		DATA LIST	REQUIREMENTS FOR SAFE TONE ON
1	Normally-on	List of Blocks	All blocks in list unoccupied
2	Normally-off	List of Blocks (Group 1, Group 2)	At least one block in Group 1 occupied. All blocks in Group 2 unoccupied.
3	Switch Guard	Switch Latch, List of Blocks (Type 1 or 2)	Switch latch set and conditions satisfied per safe tone type 1 or 2.
4	Merge Guard	Priority Latch List of Blocks (Type 1 or 2)	Priority latch status appropriate and Type 1 and 2 conditions satisfied.
5	Combination	Switch Latch, Priority Latch List of Blocks (Type 1 or 2)	Switch latch appropriate and Type 4 conditions satisfied.

e. Any previously unreported disparities are reported to the system operator via the central computer. Vehicles are prevented from entering the effected zone by closure of the corresponding Traffic Control Segment. This is not a CAS function but serves to limit the number of vehicles stopped on the guideway by the CAS.

f. The current safe tone status is output to the SPE.

6. The SPE transmits the safe tone status from the prime computer to the disparity equipment.

7. If no disparity between the hardware and software safe tone status has existed for more than 500 ms, the safe tone status is transmitted to the safe tone loop driver. A safe tone is not transmitted if such a disparity has occurred for any safe tone within the same disparity zone.

8. The safe tone status is transmitted to the safe tone loops via safe tone loop drivers. Safe tone status is displayed by indicator lights on the Test and Maintenance (T&M) Panel. During test and maintenance procedures this data can be used to determine the software safe tone status if no disparities are present or a disparity plug has been inserted.

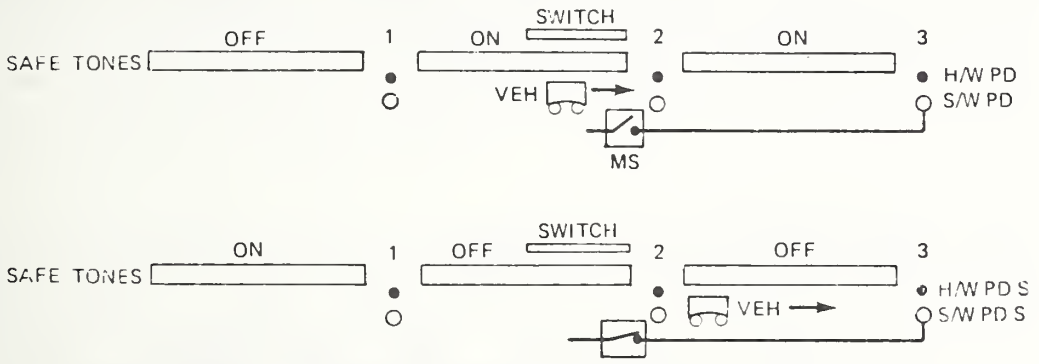
Special Software CAS Functions. As stated in Section 4.1 the software provides the following functions not performed by the hardware:

1. Slide-through protection at handover. The software CAS at each station maintains the status of the first block in the next station for each direction of travel. In the original design the handover block status was provided by a block handover message from the next station. This caused occasional disparities when timing was such that the next station would report its first block occupied before the departed station received the PD hit to clear the departed block. This created a false slide-through condition preventing the software from clearing the departed block. This problem was eliminated by allowing the software in the departed station to set the handover block occupied based upon activation of the handover PD. The next station now provides only a block clear message.

2. Detection of false switch verification. Since the switch latch received by software is set without regard to block occupancy, the software can detect a failure which causes switch verification with no vehicle present. A special software task checks for false verification once every 2 seconds. If a switch latch is set and the required block is not occupied, the software creates a disparity by turning on a normally-off safe tone and notifies the central operation. This disparity removes all safe tones from the corresponding zone thereby stopping all approaching vehicles.

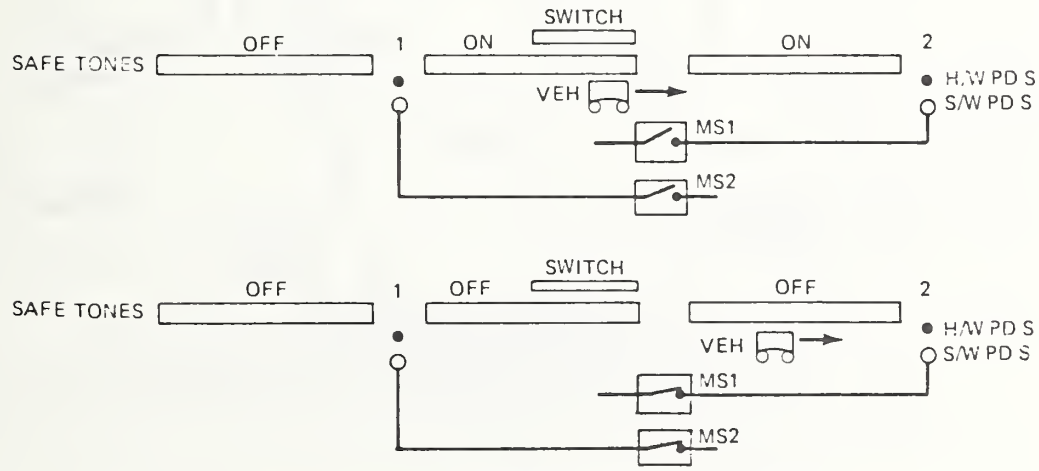
3. Steering runout protection. Activation of the steering runout switch creates a false PD hit for the software CAS. Runout switches are connected as shown in Figure 4-19. The connections are such that the normal CAS logic will remove the safe tone under the vehicle without clearing the block occupied by the vehicle. Thus, the vehicle and trailing vehicles are stopped without depending upon disparity detection. Redundant protection is provided since a disparity will occur. No special CAS logic is required for this protection.

A. SWITCH GUARD LOOP IN BLOCK DOWNSTREAM OF SWITCH LOOP



MS (MECHANICAL SAFETY SWITCH) IS ACTIVATED BEFORE VEHICLE HITS PD2

B. SWITCH GUARD LOOP IN SAME BLOCK WITH SWITCH LOOP



MS1 IS ACTIVATED BEFORE MS2

FIGURE 4-19. INSTALLATION OF RUNOUT SWITCH

4.3.4 Firmware CAS

A trade study performed at the start of Phase II concluded that a microprocessor could be programmed to perform the hardware CAS function at reduced cost with improved reliability and maintainability. The study was based upon use of an Intel 8080 microprocessor. As a result of the study and follow-up analysis, the hardware CAS function is performed by Intel 8080 microprocessors in all stations except Beechurst and Walnut. The Phase IB hardwired CAS was retained at Beechurst and Walnut since virtually no change was required for Phase II. Microprocessors were selected for Maintenance and Engineering where guideway changes led to major CAS revision, and for Towers and Medical Center which were new stations. The CAS microprocessor is a "plug-in" substitute for hardware logic. (See Figure 4-20.)

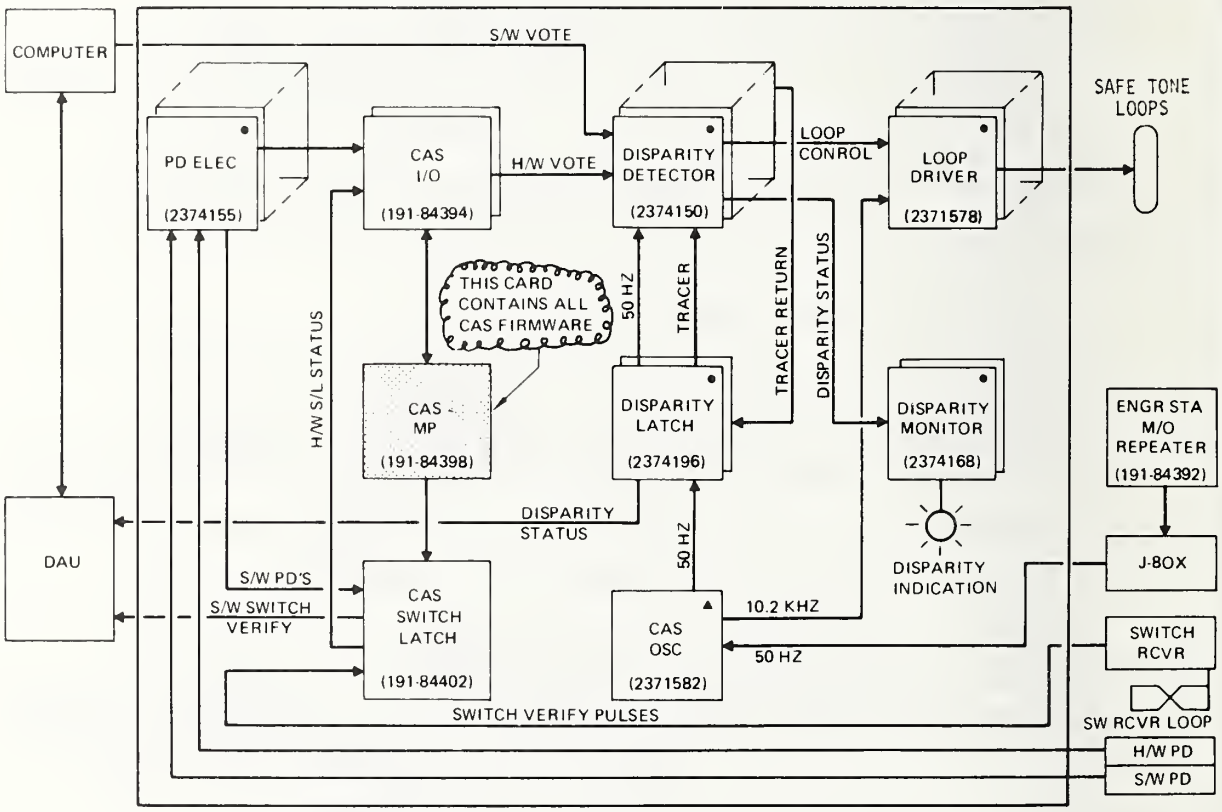


FIGURE 4-20. CAS SYSTEM COMPONENTS

Microprocessor System Description. The BOEING ESD Standard 8080 Microprocessor card is the nucleus of the CAS System. The program is designated firmware because it is stored in a read-only memory (ROM or EPROM) as opposed to software which is normally kept in read-write memories (RAM). The CAS operational firmware determines that system changes are necessary as a result of presence detector "hit" or Switch Verify signals. The system changes are determined through the CAS logic equations. The result of the equation solutions appears in the form of safe tone outputs or switch latch card control outputs.

The microprocessor card consists of an 8080A CPU, 1K of RAM, 4K of Eraseable Programmable Read-Only Memory (EPROM), a serial I/O channel, and a parallel I/O channel. Figure 4-21 illustrates the components of the CAS Microprocessor card together with the two cards directly addressed by the microprocessor.

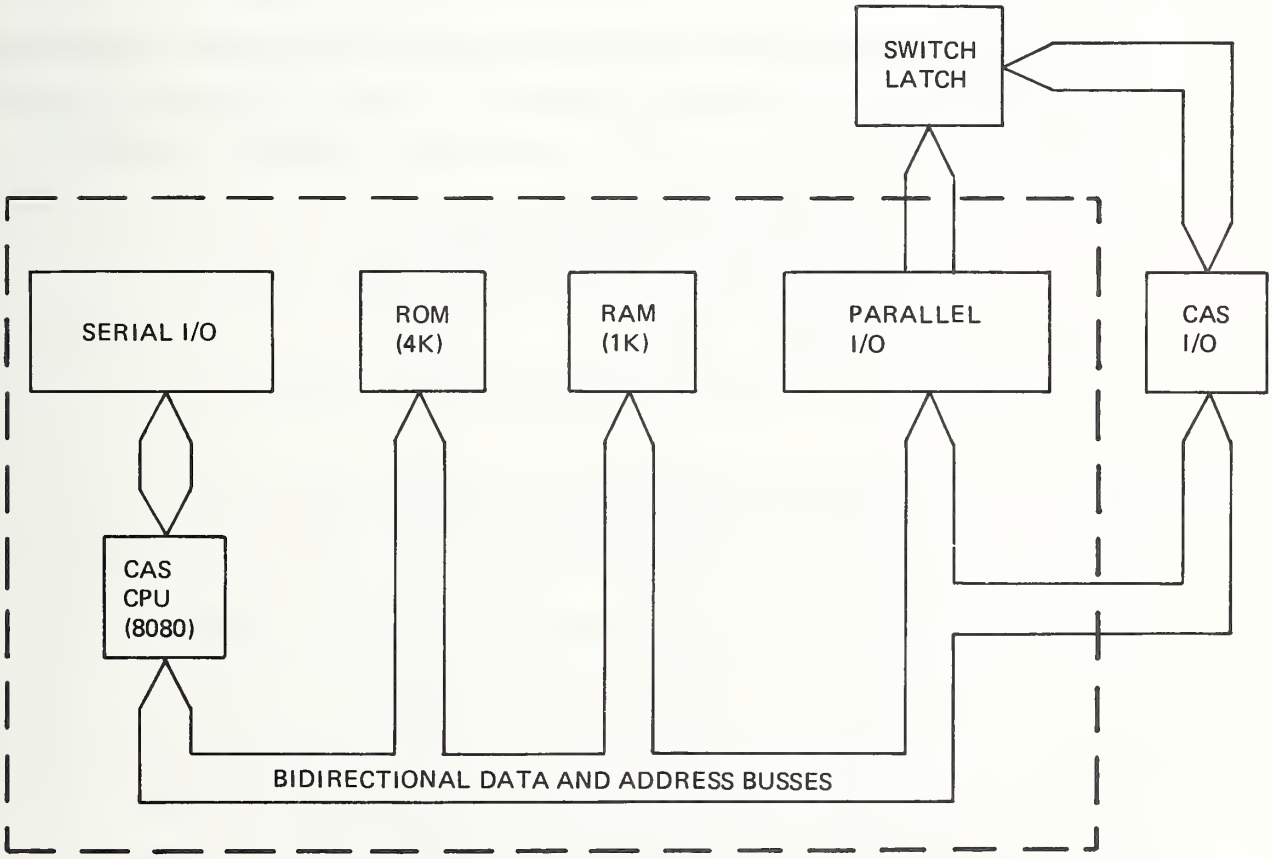


FIGURE 4-21. CAS CONTROL SUBSYSTEM BLOCK DIAGRAM

The RAM is used for storage of variable data during the CAS operation. The EPROMs contain all the programs and the constant portions of the data base assuring that the firmware will not be changed during CAS operation because of program error. The Serial I/O channel is used to maintain either a run status light or a teletype console device. The Parallel I/O channel on the microprocessor card is used only to communicate with the switch latch cards.

Most of the 8080 microprocessor interfaces connect to the rest of the CAS system through the Input/Output (I/O) cards and the Switch Latch cards. PD signals are triggered by the vehicle on the track and are latched at the I/O card inputs. After processing by the firmware program is complete, the safe tone outputs pass to the Disparity Detector and Control Gate and form the "hardware" vote. The Switch Latch control lines interface the Switch Latch card with the microprocessor and are used either to enable or to disable the Hardware switch verify counters.

The I/O card-microprocessor combination essentially performs the function of multiplexing and processing the parallel input PD lines and demultiplexing the safe tone and switch latch control outputs. Table 4-4 lists interface signals accessible to the firmware.

TABLE 4-4. INTERFACE SIGNALS

Input/Output (with respect to CPU Chip)	Signal Name	Signal Type
Input	Presence Detector	Pulse tpw - 1ms
Input	Switch Verify	Level
Input	Reset Switch	Level
Input	Reset Zone 6 Switch	Level
Input	Test Switch	Level
Input	TTY Connected	Level
Input	Station ID	Level
Input	Serial I/O	Pulses
Output	Safe tone	Level
Output	Switch Latch Control	Level
Output	Serial I/O	Pulses
Output	Run Light	Level
Output	PD Input Latch Clear	Pulse
Output	Switch Latch Input Clear	Pulse
Output	I/O Control Port	-

The functional requirements of the firmware CAS are allocated as follows:

Operational Program Component.

1. Provide safe tone control output levels per logic equations.

2. Provide all safe tone control outputs in a time period - 500 ms from the time a PD is "hit".

3. All required firmware must fit into the 4K EPROM available on the ESD 8080 microprocessor board.

4. Insure that the time between any PD "read" and its associated PD I/O card latch "clear" is less than 1 ms.

Self-test Program Component. Provide limited CPU card self-test capability for the purpose of determining if the CPU card is faulty.

Monitor Component.

1. Provide a teletype console interface with CAS microprocessor to aid in the verification of F/W.

2. Use the ESD standard microprocessor monitor, BOEMON.

4.3.4.1 CAS Program Design and Development Approach. The CAS operational firmware is designed to be data base driven. The intent is to change only the unique data base EPROMs in order to configure the firmware for each station. With this approach, it is only necessary to change two of the four EPROMs in order to configure each station.

The program is the same at all stations except Maintenance. At Maintenance, there are two block reset equations which do not fit the format requirements of the general-purpose equation-solving routines. Rather than change the general-purpose routines to include these formats which would cause an unnecessary increase in program size, complexity, and

general overhead, the two equations are solved by "brute force" in a special subroutine. With the exception of these two equations, all other CAS logic equations can be solved with the general-purpose routines.

The firmware operates in a polling mode and therefore eliminates the hardware and software complications associated with interrupt-driven systems. The polling technique is consistent with the closed loop "constant cycle time" approach used to generate the operational firmware. With this approach, all equations are solved and results are output every cycle. The worst case timing depends only on station size and not on vehicle loading. PD hits and switch verify signals do not drive the firmware but are used simply as parameters in the logic equations.

As implemented in the firmware, the switch verify equations are used to enable and disable a switch latch card counter. The "switch verified" signal is hardware-generated and can occur only after the switch latch card counter has been enabled under firmware control. When a switch latch clear PD is hit, the associated switch latch counter is disabled and the switch latch is cleared (i.e., set to "not verified"). The switch verify set equations solved by the firmware contain only the Block terms from the switch latch equations. The firmware and switch latch card together perform the AND function given in the equation. The switch latch terms found in the safe tone equations are direct inputs from the switch latch card via the CAS I/O cards. A "true" results only if the counter has been enabled by the firmware AND the switch latch counter has received seven "switch verify" pulses.

The firmware was developed using the Boeing Mini-Time Sharing (MTS) system for program assembly, editing, file management, and cassette tape generation. The object code on cassette tape was then loaded into the RAM Board in the firmware Breadboard Development tool using the Boeing Monitor program (BOEMON). From this point the firmware was debugged using operational hardware Breadboards and the Monitor program. The development tools allow the programmer to set PDs, switch latches, issue reset command, and read safe tones in order to test the firmware in a variety of states. The RAM allows debugging to proceed

quickly and easily. There is no need to transfer programs to EPROM until they are completely debugged.

Even though the CAS firmware was developed on MTS, it is not dependent on MTS and the programs may be maintained or developed on any standard or compatible Intel 8080 support system.

4.3.4.2 Module Design Description. The CAS firmware is divided into three major modules:

1. CAS Operational Program,

2. CAS Self-test Program,

3. Boeing Monitor Program (BOEMON).

CAS Operational Program. The performance of "hardware" CAS is controlled by the CAS firmware which consists of five subfunctions or tasks:

1. Executive,

2. Input or Loading,

3. Block and Switch Latch Set/Reset,

4. Priority and Safetone Set/Reset,

5. Output.

The executive routine controls program flow and calls subroutines which perform the following tasks: 1) input and format the necessary switch latch and Presence Detector data for the solution of the CAS logic equations, 2) input and interpret the various system control inputs (i.e., test active, RESET, TTY active, station ID), 3) solve the CAS logic equations, 4) toggle the CAS running light, 5) format and output switch latch card control signals, and 6) format and output safe tone

status. The executive routine calls the various subroutines necessary for system operation.

The Input or Load routines read and clear the input latches on the I/O cards. They also convert the packed input bits into data bytes and store them in RAM. The system control inputs are tested by the executive routine and appropriate program branches occur as required.

The CAS logic equations are solved by the equation solving routines which "read" the CAS data base, combine the terms of the equations per the data base information, and store the solutions on the RAM.

The switch latch card control signals are generated through solution of the switch verify reset and set equations. The results are then formatted and output to the switch latch card.

The results of the safe tone equation solutions are formatted for output by pack routines which convert the word oriented format into bits that are necessary for safe tone control. Then results are output and automatically latched.

Safe tone equations are solved by a single subroutine. This is achieved by expressing each safe tone equation in terms of a single generalization equation:

$$S = A \bullet B \bullet C$$

where

$$A = A_1 + A_2 + \ldots$$

$$B = B_1 \bullet B_2 \ldots$$

$$C = \overline{C_1} \bullet \overline{C_2} \ldots$$

The equation states that a safe tone is on (true) if each of 3 terms is true. (Terms which are not applicable are omitted.) The first term is true if at least one of its elements is true. The second term is true if all its elements are true. The third term is true if all its elements are false (off). The elements for the first two terms (A and B) are blocks, switch latches, and priority latches.

The elements for the third term are blocks and priority latches. For example:

Let $S = SL \cdot \overline{PL} \cdot (B_1 + B_2) \cdot \overline{B_3} \cdot \overline{B_4}$

Then $A = B_1 + B_2$ (block 1 or block 2 occupied)

$B = SL$ (switch latch set)

$C = \overline{PL} \cdot \overline{B_3} \cdot \overline{B_4}$ (Priority latch and blocks 1 and 2 clear)

The data for a given safe tone equation consists of a list of addresses pointing to the status for each element in each term. The list has zero length for terms which do not apply. This approach significantly differs from the approach used for the software CAS thereby minimizing the probability of identical errors in the two systems. The two systems were developed independently to encourage such diversity.

CAS Self Test Program. The CAS self-test is designed to fault isolate to the CPU card level since this is the most important card in the CAS system. The test is accomplished through:

1. EPROM checksum test,
2. CPU chip instruction and register check,
3. CPU card - I/O card bus test, and
4. A "walking 1" RAM test which does not destroy the data in memory.

The EPROM checksum test sums all EPROM memory locations and compares the result with a known good checksum. The CPU test checks the 8080 chip instructions and registers. The BUS test checks the common bus between the I/O cards and the CPU card to a limited extent. It writes to two locations on the I/O cards, and if either location can be read correctly, the bus is assumed to be okay.

Boeing Monitor Program (BOEMON). BOEMON is the monitor program supplied with the Boeing standard microcomputer card. Its purpose is to provide user access to a console device during the checkout of system hardware and programs.

BOEMON was used for development, for verification program functions, and for validation of the system. It is not used in normal operation but is included in the production CAS to support firmware modification if required.

4.3.5 Disparity Equipment

The disparity equipment consists of disparity detectors which remove safe tones when a disparity is sensed and disparity latch which will not allow the safe tones to be restored until corrective action has been taken.

4.3.5.1 Disparity Detectors. The following discussion references the simplified schematic given in Figure 4-22.

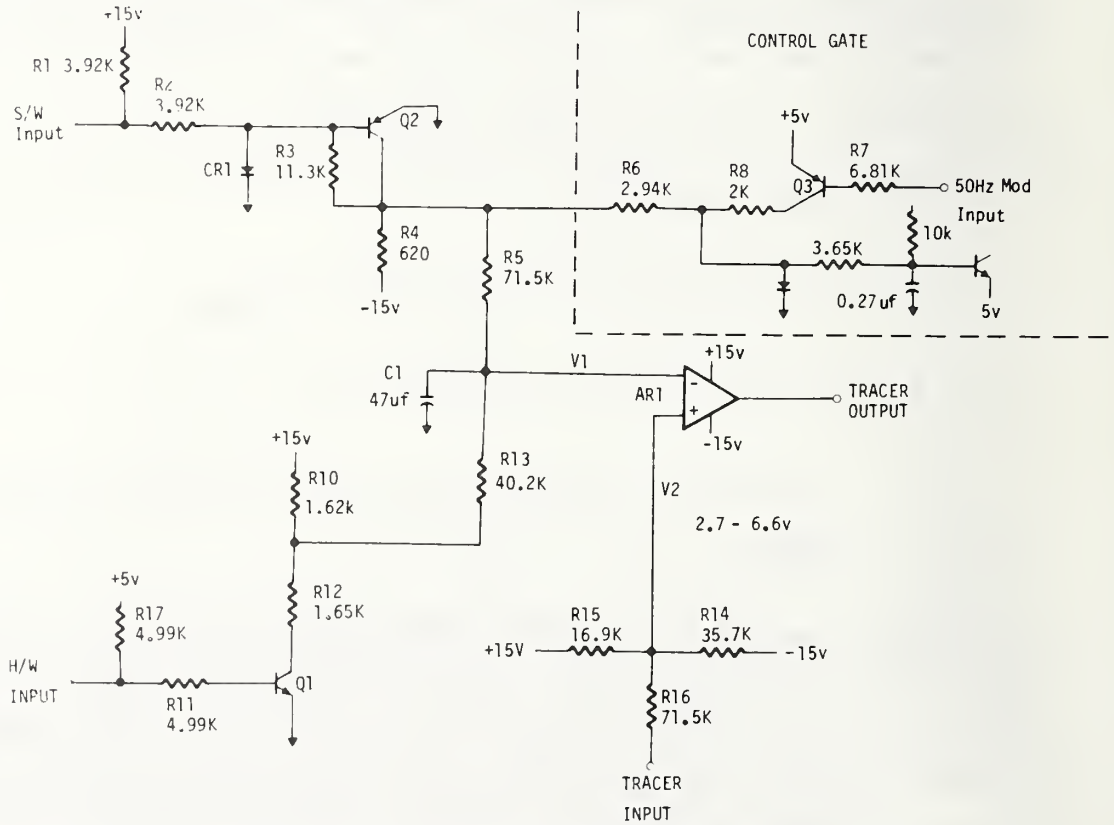


FIGURE 4-22. DISPARITY DETECTOR AND CONTROL GATE

There are four disparity detectors per card (as well as four control gates).

Resistors R14, R15, and R16 attenuate and level shift the tracer input from the last stage (AR2). The tracer swing at the non-inverting input of AR1 is nominally 2.7 v to 6.6 v. Therefore, the bias at the inverting input must be in this range for the tracer to continue. The bias at this point will be at four different levels corresponding to the four possible input states. These bias levels and the corresponding input states are listed below.

Software Input	Hardware Input	Bias at AR1(-)
0	0	9.5v
0	1	4.8v
1	0	3.9v
1	1	-0.7v

Notice that when the software and hardware inputs are complements (agreement), the bias level is between 2.7 and 6.6v, and, therefore, the tracer continues. These bias levels are mostly dependent on the voltage divider composed of R5 and R13 and on the states of Q1 and Q2. The voltage at Q2's collector is nominally 0v or -15v. The voltage between R13 and R12 is nominally 15 or 7.5v.

Capacitor C1 permits temporary disparities allowing for the software and hardware computation times. The following table lists the transition times for changes from agreement to disagreement in the hardware and software votes. These times are grace periods before the disparity detector interrupts the tracer.

Initial Input		Next Input		Nominal Bias	Threshold Voltage	Time
S/W	H/W	S/W	H/W			
0	1	0	0	4.8v	6.6v	0.54s
0	1	1	1	4.8v	2.7v	0.64s
1	0	0	0	3.9v	6.6v	0.82s
1	0	1	1	3.9v	2.7v	0.46s

Four control gates also appear on the disparity detector cards. Figure 4-22 includes an example of a control gate. Q3's emitter is held at +5v. Therefore, when Q2 is on (software = 1 = modulation on), the 50 Hz modulation applied to Q3's base through R7 is available at the R6/R8 junction. This output drives the loop driver.

4.3.5.2 Disparity Latch. The following discussion references the simplified schematic given in Figure 4-23.

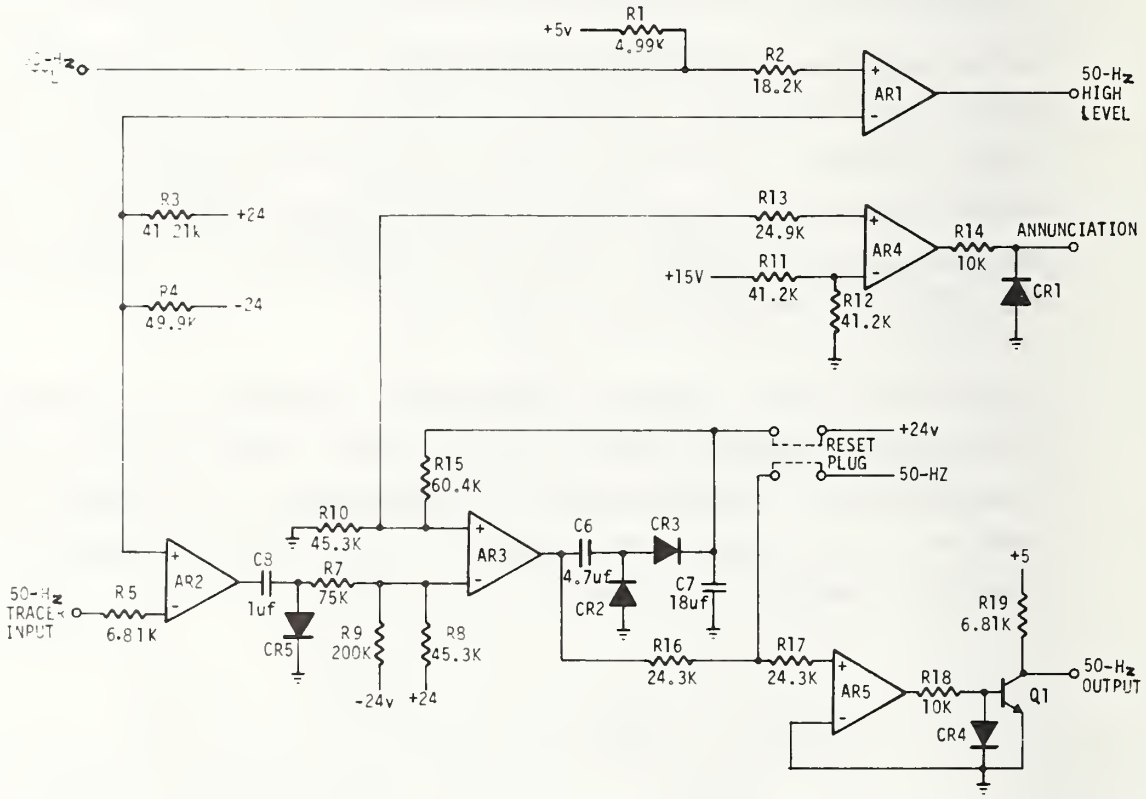


FIGURE 4-23. SIMPLIFIED SCHEMATIC OF DISPARITY LATCH

The 50 Hz tracer from the last disparity detector (in a zone string) enters the disparity latch at the inverting input of AR2. The high level (±14v) tracer is compared against a 2.3v bias on the non-inverting input of AR2. This bias is developed by R3 and R4. The network composed of C8, CR5, R7, R8, and R9 converts the 50 Hz ±14v output of AR2 to an attenuated and level shifted square wave at the inverting input of AR3 which swings from approximately +9 to +15 v. The output of AR3 will swing ±14v at 50 Hz if its non-inverting input is biased between +9 and +15 v. The output of AR3 drives a voltage doubler composed of C6, CR2, CR3, and C7. The output of the voltage doubler (28 v) is attenuated (by R10 and R15) to 12v. This bias is between 9 and 15v, which is the requirement to enable AR3 to switch. Notice that the bias at the non-inverting input of AR3 is provided by AR3. At turn-on, this bias is provided by a +24v reset applied to C7, which permits AR3 to switch and provide its own bias. If (after a reset) the input from AR2 is lost long enough for C7 to discharge below 21v (9v at AR3), then AR3 will not switch. This action removes drive from AR5 and Q1 which removes the 50 Hz tracer from the disparity detector control gate. Capacitor C7 will discharge from 28v (nominal voltage doubler output) to 21v (9v at AR3) through R10 and R15 in 0.5 seconds. Therefore, the tracer can be lost for 0.5 seconds before the disparity latch removes the 50 Hz tracer from the disparity detector control gate. Op Amp AR1 converts the TTL level signal from the 50 Hz master oscillator to a high level drive for the first disparity detector (in a zone string). The TTL level input must swing above and below the bias at the inverting input (2.3v from divider action of R3 and R4).

Op amp AR4 compares the AR3 non-inverting input bias against 7.5v derived from the R11 and R12 voltage divider. If the AR3 bias falls below this level, the output of AR4 goes to -14v. Diode CR1 clamps this to one diode drop below ground. This input to the monitor produces the latch annunciation. Transistor Q1 provides a TTL level signal to the disparity detector control gates. Op amp AR5 acts as a buffer between Q1 and AR3 (high impedance load for AR3).

Note that the reset plug over-rides the disparity latch since it not only resets the latch (24v connection) but also provides 50 Hz to AR5 and Q1 which drives the disparity detector control gates.

4.3.6 Safe Tone Subsystem

Safe tones are transmitted to vehicles by inductive communication through safe tone loops imbedded in the guideway. Safe tone loop layout considerations are discussed in Section 4.2.2 of this report.

The safe tone, a "safe to proceed" tone, is received by redundant receivers in the VCCS (Vehicle control and communication subsystem). Loss of the safe tone for longer than 150 ms results in an emergency brake stop by the vehicle.

The original CAS system had the speed tones performing the dual function of speed and safe tone by commanding an emergency brake stop with tone removal. The goal was to provide a system with 20-db signal-to-noise ratio using a receiver with 50-ms integration. One later version of the concept used two frequencies for safe tone; 10.2 kHz was "safe to proceed" in the forward direction, and 13.3 kHz was "safe to proceed" in the reverse direction. Each tone was 100 percent modulated by a 50-Hz square wave.

The Phase IA system specification describes a system consisting of only one tone (10.2 kHz, 50-Hz modulated) with the transmitter providing an output level that will ensure a minimum signal-to-noise ratio design goal of 20 db with 50-ms integration measured at the vehicle-borne receiver input. This is based on noise environments of MIL-STD-462 and NBS circular 461A when the vehicle-borne receiving loop is over the guideway tone loop. Self-test features are deleted. One of the ancillary requirements not specifically mentioned is to ensure that the residual safe tone in an "off" loop remains well below the receiver detection threshold.

In Phase IA numerous tone dropout problems were encountered. In particular, it was found that certain crossover spacings necessitated by the loop-to-loop balancing criteria resulted in crossovers under each section of the dual receive antenna at the same instant causing loss of safe tone in both receivers and a resulting emergency brake stop. Normally, crossovers or dropouts due to loop ends should not affect operation because one receiver should always receive safe tone due to the antenna offsets. Also, to avoid loop boundary problems all loops in a given station were in sync. There was a 10.2-kHz master oscillator for carrier and a 50-Hz master oscillator for supplying modulation. Therefore, in theory, a "handover" problem should have existed at the boundary between two stations, though records do not indicate a phase IA problem in this area, probably due to the forgiving nature of the Phase IA VCCS design. A recognized signal margin problem did exist, however, due in part to vehicle antenna-tracking problems and in part to the low level of transmitted signal on the loops. Some investigation was made into methods to increase the Phase IA CAS loop driver output (such as reducing termination resistors to from 60 to 40 ohms and increasing the voltage to the output stage); however, none of these fixes were adopted.

A guideway signal study done prior to Phase IB design indicated that the Phase IA system had a very small positive margin on the safe tone. Levels 6 db below the target were measured. As a result of the marginal situation, the new VCCS was made more sensitive in an attempt to recoup some of the lost margin.

One of the very first problems encountered in Phase IB was the loss of safe tone at station handover points due to the modulation (50 Hz) of the two stations being out of sync. The out-of-sync modulation caused a ringdown of the VCCS active filter and subsequent loss of safe tone and activation of vehicle braking. The problem was rectified by adding a 50-Hz master oscillator at the central control facility and by providing synchronization to slave oscillator cards in all of the other stations.

Another area of concern to all Phase IB communication systems was noise, and the safe tone system was no exception. Noise at the safe tone frequencies was found at switches and on the station safety ground. Vehicle-generated noise also was thought to be a problem. Several solutions were implemented to reduce noise in the 10.2-kHz bandpass. One solution was the implementation of the bifilar antenna to reduce noise coupling from the vehicle power and ground wiring. Noise from the station ground (fourth rail safety ground) was further reduced by inserting a 10.2-kHz notch filter in the fourth rail safety ground within the vehicle. Other contributors to the problem were (1) insufficient signal on the guideway and (2) wide variability in receiver thresholds. Therefore, the VCCS sensitivity was modified, in part, by hand selecting the phase lock loops used in the receiver such that the total vehicle-to-vehicle variation was reduced.

As previously mentioned, residual safe tone in "off" loops was also of concern because it could prevent a vehicle from stopping if it were detected by the VCCS. Surveys were made, and some areas were found to be high. The out-of-tolerance loops were caused by improper installation (crossovers out of position, etc.) or by problems related to a station wire shield grounding. As a result, the grounding scheme at that station was reworked, and all loop fed cable shields were tied directly to the station ground at the J-box; this corrected the problem.

Crosscoupling was also found in merge and demerge areas due to the merging or demerging loop signal being received off the side lobe of the vehicle antenna. Investigation revealed that due to loop and antenna geometry, the crosscoupled signal might be detected and provide interference until the loop-to-loop spacing in the merge or demerge exceeded 15 in. Some loops were modified where feasible.

Stopping margins were analyzed also. It was found that stopping margins were safe, even with the crosscoupling.

Figure 4-24 shows the safe tone subsystem. The figure is applicable for Phase IA/IB and Phase II systems. No changes were made to the station electronics for this subsystem in Phase II.

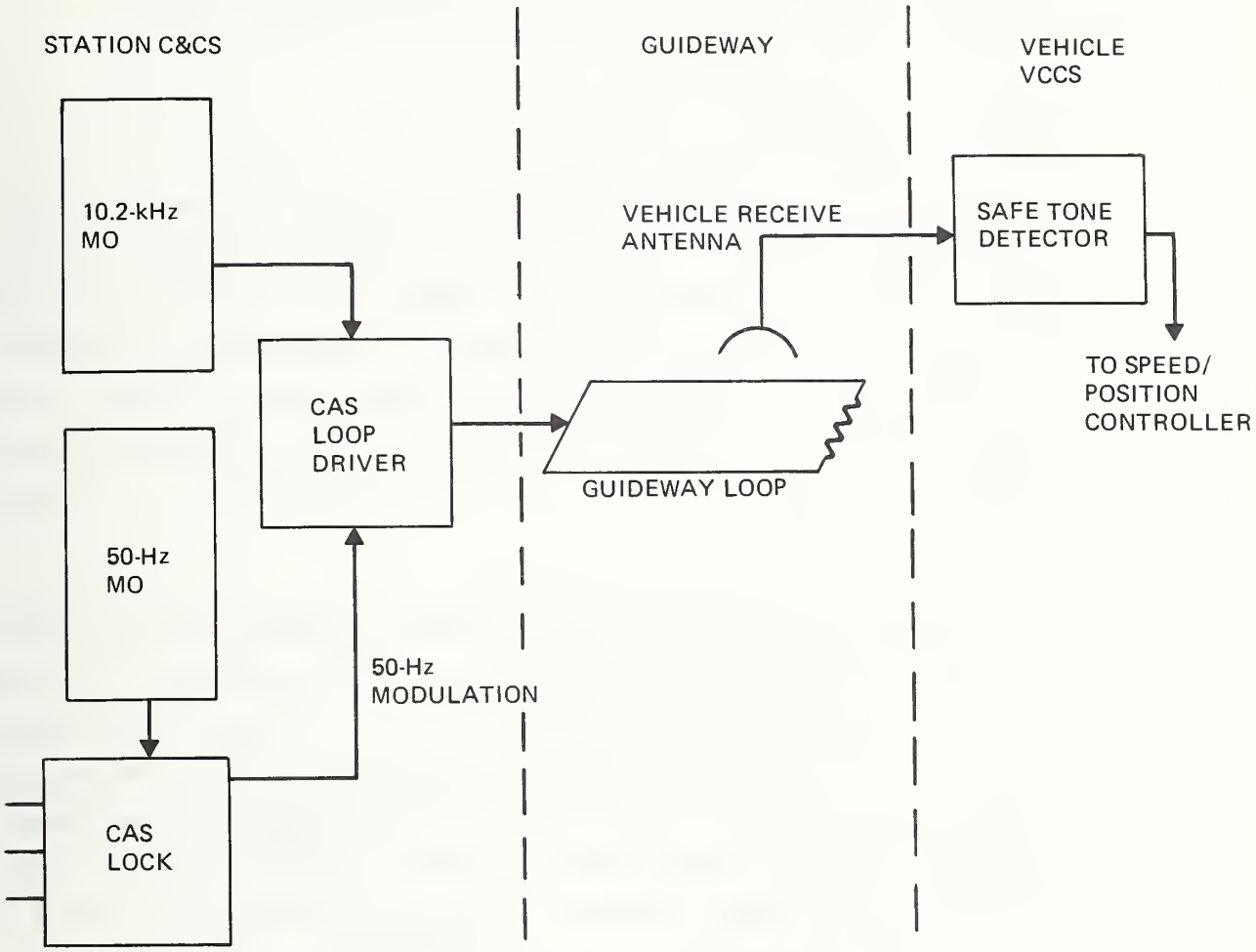


FIGURE 4-24. SAFE TONE SUBSYSTEM

5. CAS ASSESSMENT

The following paragraphs present an assessment of the CAS. They include an anlaysis of the CAS and describe the tests performed from initial subsystem tests to final checkout of the installed system.

5.1 ANALYSIS

This section presents an examination of the CAS in terms of safety. Both the CAS concept and its implementation are inherently safe by their nature. The concept involves checked redundancy. The implementation employs a low frequency modulated carrier, which makes it extremely improbable that a failure, or a group of undetected failures, or self-oscillation of a unit would produce exactly the right combination of carrier frequency, modulation frequency and amplitude to be interpreted in an unsafe manner.

Most failures would be safe even if a dual CAS were not used. This is because a conceptually fail-safe approach has been used. For example, absence of a valid safe tone signal will stop vehicles. Thus, most safe tone transmission and detection failures are safe since vehicles cannot proceed. Also a missed PD is safe since this failure leaves a trailing block occupied and/or will not allow the vehicle to enter an unprotected guideway segment. This was discussed in Section 4.1.

The following examination, derived from safety studies performed by Bendix at the start of Phase IB, concentrates on failures which require analysis to verify safety. Each potential failure examined is regarded as a candidate for unsafe analysis. Analysis of each failure either shows the failure to be safe or the probability of failure to be low relative to collision avoidance safety standards, such as those of the railroad industry.

5.1.1 CAS Examination

The principal safety feature of the CAS is checked redundancy wherein two functionaly identical systems perform the same manipulations of the same input data. Their outputs are checked. If the outputs disagree, the system is brought to a halt in a safe manner. Nearly all potentially hazardous signals are checked by this means. However, the nature of the logical operations is such that some signals cannot be easily checked. For each of these signals the unsafe failure conditions were determined, and all component failures which could possibly cause the unsafe signal were identified. The failure rates were then added yielding the rate of undetected failures for the hardware logic. Unsafe failures will not occur unless both the hardware and software CAS fail on the same logic operation with the same failed output state, affecting the same point on the guideway.

Figure 5-1 presents a quantitative fault tree which summarizes the results of the analyses contained in the following paragraphs.

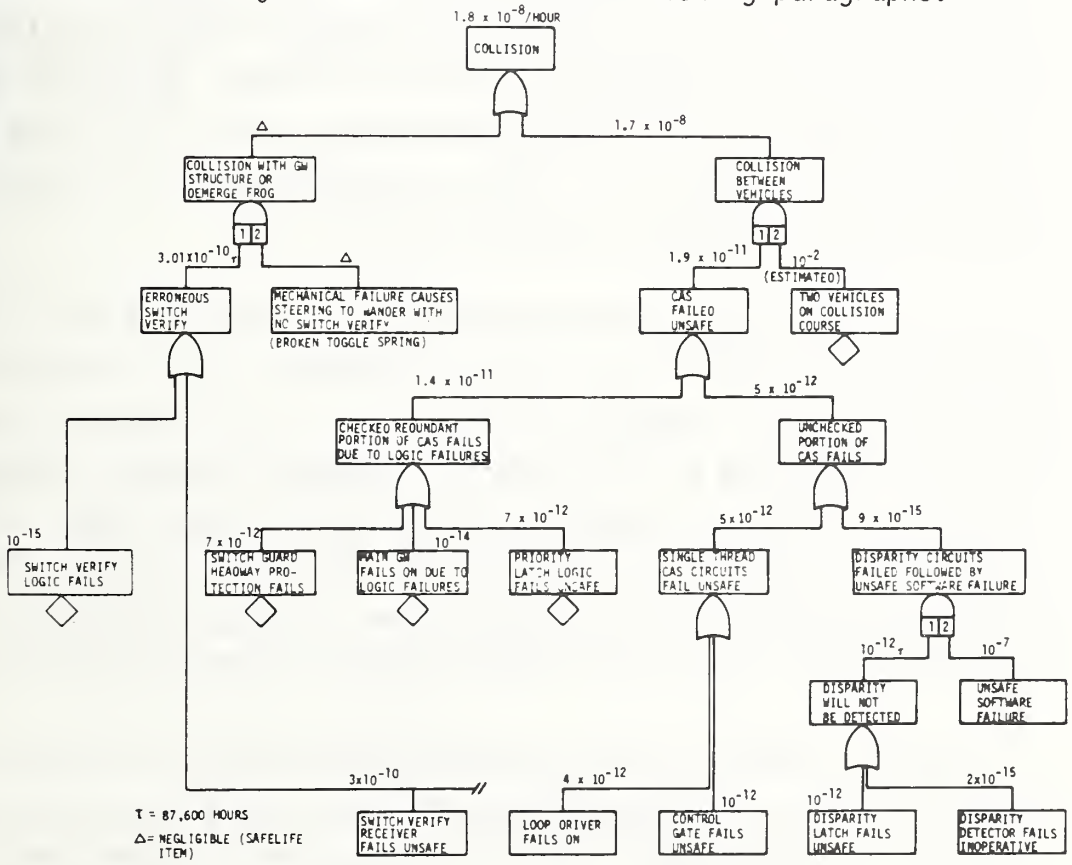


FIGURE 5-1. CAS FAULT TREE

It combines the probability of unsafe failures in the checked redundant logic (Section 5.1.1.1) and in the unchecked fail-safe circuits (Section 5.1.1.2). It should be noted that although the switch verify CAS circuits are part of the CAS by design and were analyzed as such, they play no part in preventing collision between vehicles. Provided the vehicle is steering on one side or the other, there is no hazard. If the vehicle steering system fails in an in-between position, however, the vehicle may collide with the guideway structure or the frog at demerges. The failure rates in Figure 5-1 were taken from the succeeding analyses. The fault tree is evaluated using the "lamda-tau" (λ-τ) method, in which λ is the failure rate and τ is the "repair time" or duration of the failure. The estimate is conservative in that all τs on the fault tree were assumed to be 87,600 hours (10 years). That is, no failure detection or repair is assumed.

The assessment shows the CAS to be extremely safe. The failure rate for loss of collision protection is only 2×10^{-11} per hour. This compares favorably with failure rates of 10^{-8} per hour traditionally accepted by the railroad industry. Allowing for a vehicle control failure rate of 10^{-2} (potential collisions per hour) and no CAS repair, the maximum probability of collision is estimated to be 2×10^{-8} per hour after 10 years of operation. This is almost four orders of magnitude better than the Morgantown safety criteria.

5.1.1.1 System Logic. The checked redundant portion of the CAS, by its nature, can fail unsafe only if undetected logic failures occur. For the purposes of analysis, it is convenient to divide the logic circuitry into three distinct groups. These are: the main guideway in which the same logical operations are repeated for each block, switch verify logic circuits, and priority logic flip-flop circuits. The following paragraphs analyze typical cases of each, and Section 5.1.1.4 presents a fault tree of the checked redundant portion of the CAS.

It should be noted that any failure mode which results in a safe tone being OFF when it should be ON and which does not produce other (unsafe) conditions is always safe. This is irrespective of whether the failure

is detected immediately (i.e., by a disparity) or whether it remains failed until a vehicle enters the loop, in which case the vehicle simply stops.

5.1.1.1.1 Main Guideway Logic. The elements of the hardware CAS block occupancy logic are shown in Figure 5-2.

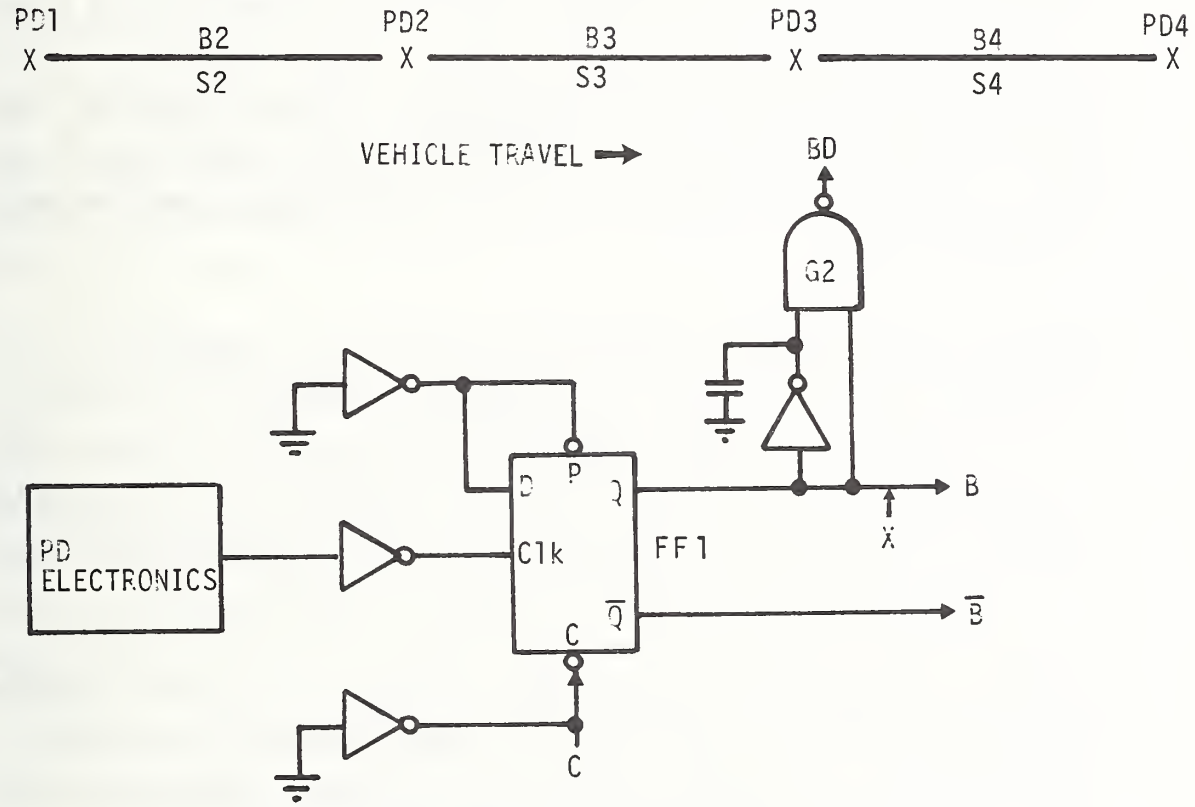


FIGURE 5-2. MAIN GUIDEWAY LOGIC

Typically, a safe tone is ON if the block ahead is unoccupied. A block is set occupied by activation of the entry PD; it is reset (cleared) by activation of the exit PD if the block ahead was clear.

Using notation of Figure 5-2, the conditions can be expressed as follows:

$$S2 = B3, \quad B3 = PD3 \cdot B4,$$

or $S2 = B3$ (safetone OFF),

and $S2 = PD3 \cdot B4$ (safetone ON).

The disparity detector compares S from the software CAS logic with S from the hardware. Thus, the disparity detector monitors the same wire (Q in Figure 5-2) that generates the reset (clear) for the previous block. Any failure or malfunction which immediately causes a change in the B output is detected by the disparity detector, and the system is rendered safe by removal of safe tone modulation. Any failure or malfunction which does not immediately change the output is not immediately detected and is potentially unsafe. Such failures are analyzed below.

Block Occupancy Logic Fails Set (Occupied). In normal operation, the output of B of FF1 is low (i.e., the block is not occupied and S1 is ON). Any failure which makes B = 1 is thus immediately detected and is rendered safe.

However, during the short interval that the block is occupied B = 1, and the postulated failure is not immediately detected if it occurs while the block is occupied. When the vehicles leave the block, the correct output is B = 0, and the failure condition, B = 1, is detected, provided a corresponding failure does not occur in the computer logic, in the same time interval that the block was occupied.

If both failures occur during the time interval, the failure condition will remain undetected. The block will remain apparently occupied although there is no longer a vehicle in the block. Since safe tone states are governed by the block occupancy ahead, the safe tone of the faulted block will turn off as the vehicle enters the next block. Since the block occupancy term remained set (i.e., the block did not clear), the safe tone behind the faulted block remains off. Thus, two safe tones are off behind the vehicle instead of the normal one. As previously stated, a fault condition which results only in a safe tone off is regarded as safe. Thus, block occupancy failing set, although not immediately discovered, is not a hazardous failure. The safe tone that is incorrectly off will remain off until the problem is rectified. It will be discovered when the next vehicle enters the off safe tone and stops.

Block Occupancy Logic Fails Reset (Clear). If the logic components of an unoccupied block fail in the clear state (B = 0 in Figure 5-2), failure will not be detected since that is its current state. A failure resulting in B = 0 is not detected until a vehicle passes, at which time B should become 1, but the postulated failure causes a disparity. In normal operation the block may be unoccupied for long periods of time. If the computer fails in a corresponding way, during the time between vehicle passings, the failure is undetected. However, when a vehicle passes a block failed B = 0, the inability of B to change to 1 will prevent reset of the previous block causing a disparity on the previous block. If this block had similarily failed (corresponding failures in the computer CAS and hardware logic), prevention of reset of the next previous block will cause a disparity.

Because the block is never set occupied, the safe tone of the previous block will not turn off, per the safe tone equation. This is an unsafe condition. If a disparity is generated in the logic of the previous block, the disparity removes the trailing safe tone (and all other safe tones in the CAS zone), and the vehicle is protected. Thus, in order to be unsafe, both the computer CAS and the hardware logic output signal must fail, and the reset signal must operate normally so that a disparity is not generated in the previous block. Referring to Figure 5-2, the postulated failure is: B = 0, but Q output of FF1 is operating normally and providing normal reset on Line BD (i.e., an open circuit at X, and B subsequently shorted to ground). (An open circuit at X, by itself, will immediately cause a disparity.)

Normally vehicles will be traveling all blocks on the guideway relatively frequently and the interval of time between vehicles (in which these three faults must occur to produce the unsafe condition) is small. These factors together make occurrence of the unsafe scenario extremely improbable. Using a conservative figure of 24 hours between vehicles, the probability of occurrence of a hazardous condition is estimated to be less than 10^{-12} per system hour.

5.1.1.1.2 Switch Verification Logic. Switch verification logic is incorporated into the CAS block logic to prevent a vehicle from proceeding beyond a switch zone unless it has confirmed switching. Representative switch logic and associated guideway loop geometry is shown in Figure 5-3.

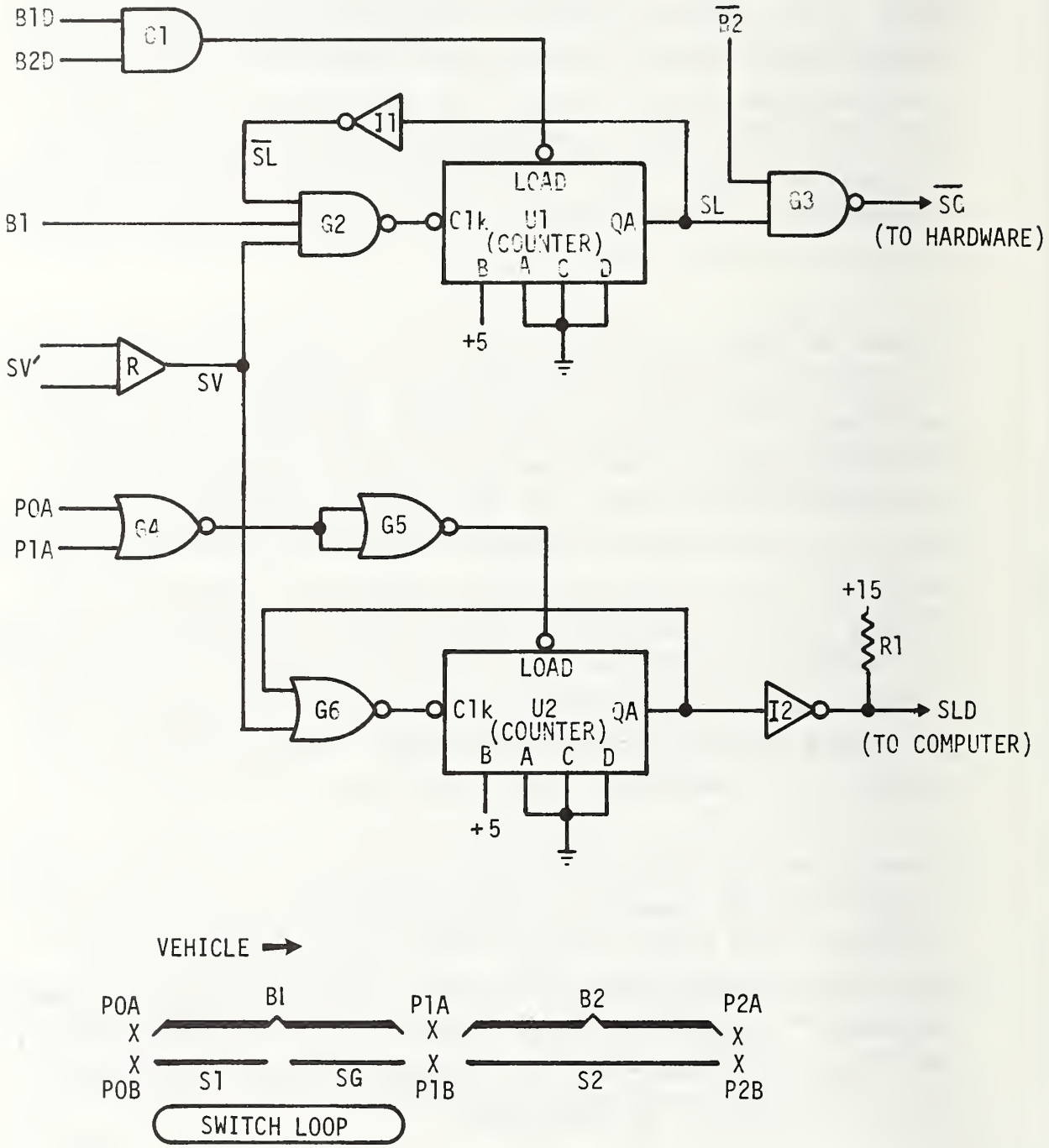


FIGURE 5-3. SWITCH VERIFICATION LOGIC

A vehicle that does not properly verify is protected by a normally-off CAS "guard" loop (SG) at the downstream end of the switch zone. This loop is turned on only when the latched switch verification signal (SL) is present and downstream headway clearance exists.

The switch verification signal from the vehicle is received by a switch verification receiver associated with each switch loop. Whenever this signal is present, the verification receiver provides an ac signal at 50 or 70 Hz to the verification logic. The verification logic then digitally integrates the signal for 7 cycles to establish valid verification. It is maintained (latched) by the verification logic until the vehicle has proceeded through the switch zone.

For the hardware CAS, the switch verification logic provides all interlock conditions using inputs from the hardware block occupancy flip-flops and associated reset pulse generator. Signals labeled B are obtained from the Q output of the flip-flop and B is obtained from the Q output. A block signal with a "D" suffix is the reset pulse derived from the transition of the Q output. (See Figure 5-2.) Conditions are imposed upon the processing of the switch verification ac signal, SV, to yield the latched signal, SL. These conditions ensure that the SL signal is reset after the vehicle passes; they also guard against the accumulation of noise in the digital integrator. In general, the conditions are (1) that the integrator be reset whenever the entrance or exit presence detector is activated, and (2) that the verification signal be accepted only if block occupancy in the switch zone is indicated. In symbolic notation the control conditions are:

$$SL = B1 \cdot SV \qquad \text{(set)},$$

$$\overline{SL} = P0 + P1 \qquad \text{(Clear)},$$

$$\text{and} \quad SG = SL \cdot B2 \qquad \text{(on)}$$

$$\overline{SG} = \overline{SL \cdot \overline{B2}} \qquad \text{(off)}.$$

For the software CAS the switch verification logic reset conditions operate on signals from the software presence detectors ("A" suffix), and the block occupancy interlocks are omitted. These interlocks are used for a software validity check of the SLD signal. The switch verify integration logic circuitry utilizes separate integrated circuit chips for the hardware and software functions.

Referring to Figure 5-3, the verification logic for hardware and software CAS operates as follows:

1. The ac signal (SV) is received by the differential receiver, R, and level converted to a pulse logic signal SV.

2. Gate G2 blocks the SV signal unless occupancy in the switch zone is indicated. It also serves to latch the circuit, after the required number (7) of verification pulses have been received, by means of the SL input.

3. U1 is a 4-bit counter (SN54197). The "load" value and clock input connections are so arranged that the QA output goes to the "7" state on the 7th SV clock input.

4. Gate G1 "ors" the reset conditions for U1, since a low is required to load, and the reset signals are true when low.

5. Gate G3 is the guard loop control gate combining the SL and headway protection block signals for the hardware logic.

6. Gates G4, G5, and G6 and counter U2 develop the software switch verification signal in a similar manner with exceptions as previously described.

7. Inverter I2 and resistor R1 invert and level shift the software signal SLD for compatibility with data acquisition inputs.

Verification Logic Fails High. Any failure of the SLD output in the high state is safe since this prevents switch verification from reaching the software logic. Any failure of the SG output in the high state is safe since it indicates the loop should remain off and will result in a disparity as soon as a vehicle enters the switch zone and verifies.

Verification Logic Fails Low. The switch verification logic hardware output is the guard loop signal which is directly disparity checked. A failure of this output signal from the loop "off" (output high) to the loop "on" (output low) state is immediately detected if the state was "off". If the failure to "on" occurs while a vehicle is in the loop and the loop should be "on", detection is deferred until the vehicle exits the loop. In either case the failure is detected with "normal" operation of the system.

Failure of the software switch verification output signal in the "true" (verify) state is potentially unsafe if undetected prior to the time a corresponding failure develops in the hardware logic. As described in Section 4.2.1.3, a failure that appears as a switch verification from an unoccupied block will create a disparity within two seconds by turning on the switch-guard loop via the software logic while the hardware switch-guard signal remains off. Thus, even if both hardware and software logic failed on, a disparity would still be created since the block is actually unoccupied. The disparity would be detected within one second. Thus, three events must occur within three seconds to cause a potentially unsafe situation. Both the hardware and software logic must fail, and a vehicle must enter the block within the three seconds. The probability of co-existence of these events in the time duration involved is remote and the Bendix study estimates it to be in the order of 10^{-15} per system hour.

Headway Protection Failure. Since switch guard loops are normally off, failure of B2 high (block unoccupied) would normally be undetected until a headway violation occurred. No hazard occurs unless the hardware and software both fail. Special monthly tests are performed to detect such failures in logic controlling normally-off safe tones. In the Morgantown system there are several variations of guideway loop geometry

at switch zones. As a result, variations exist in the number of terms in the number of blocks involved in headway protection. Based upon Bendix study, the probability of loss of headway protection is 7 X 10^{-12} per hour for the worst case.

5.1.1.1.3 Priority Flip-Flop. Whenever a number of signals are applied to an "and" gate to affect the safe tone control signal, it is possible that a failure of one or more of the input signals will be undetectable, and possibly unsafe, because they do not cause the gate output to change immediately. The logic around the priority flip-flop is typical and is utilized many times in the CAS. The basic circuit is analyzed here.

The priority flip-flop is used to assure safety if two vehicles approach a merge simultaneously. A functional block diagram is shown in Figure 5-4.

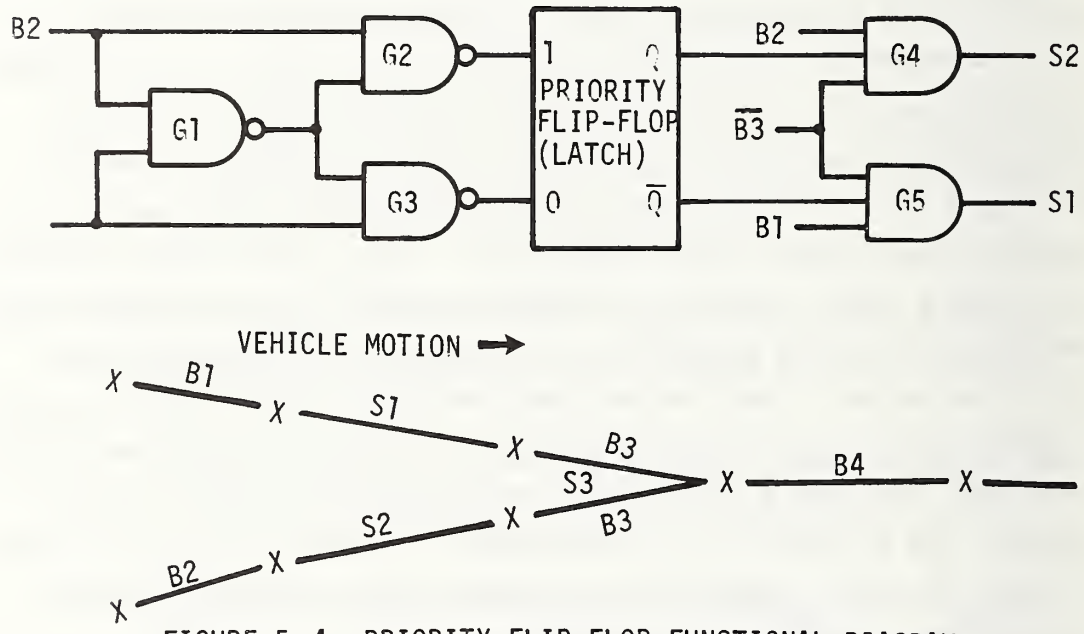


FIGURE 5-4. PRIORITY FLIP-FLOP FUNCTIONAL DIAGRAM

A vehicle approaching the merge via either leg will approach a guard block which is normally off (S1 and S2). When a vehicle is actually in the upstream block (such as B1) the corresponding guard safe tone (S1) will be turned on if: block 3 is not occupied, block 1 is occupied, and priority flip-flop output, Q = 1. (I.e., the inputs to G5 are all 1.) The priority flip-flop is set to Q = 1 when the vehicle

enters B1. However, if a second vehicle enters B2 while the first is in B1, the priority flip-flop is prevented from changing, and the second vehicle is stopped by S2 (off) since the G4 output remains off. If both vehicles enter their merge entry blocks simultaneously, the priority flip-flop is prevented from changing (by G1) and one vehicle is permitted to pass while the other is stopped.

Outputs Fail Low (Off). Any failure which causes S1 or S2 to fail low is safe whether a vehicle is present or not. One branch of the merge is then effectively closed (safe tone off) and a collision cannot occur. Any vehicle entering the failed branch will simply stop due to loss of safe tone.

Output Fail High (On). Any failure which causes S1 or S2 to fail high is potentially unsafe except for the fact that it is detected immediately. The hardware CAS disagrees with the software CAS and a disparity results turning all safe tones off in that CAS zone. Both the hardware CAS and the software CAS would have to fail in a corresponding manner within the half second window necessary to obtain a disparity. The probability of two independent failures occurring in this small time duration is negligible.

Input Logic Fails. Failure of logic inputs to gates G5 and G4 may or may not be unsafe, depending on the mode of failure and the time of detection. These are examined below. In the context of the following discussions, "Normal" operation corresponds to system operation without headway or merge violation. If failure is detected in normal operation, the zone will have safe tone removed, the system is safe, and no other analysis is required. If not, the effect of added system failures (headway violation, or software CAS failure) must be considered.

B1 (or B2) Fail Low. This is the same as S1 (or S2) failing low. The safe tone in the failed branch cannot turn on and is, therefore, safe. It will be detected in normal operation when a vehicle arrives and a disparity occurs.

B1 (or B2) Fail High. This mode of failure, in which the block is erroneously represented as occupied, is safe. The safe tone logic of the previous block on the guideway will command that safe tone off, a disparity will result within one second of the failure, and a vehicle will be unable to enter the merge.

$\overline{Q}$ (or Q) Fails Low. This is similar to B1 or S1 failing low. In this case, at least one safe tone cannot be turned on and the system is safe. It will be discovered in system normal operation when a vehicle arrives and a disparity is created.

$\overline{Q}$ (or Q) Fails High. This mode of failure would be unsafe were it not for the existence of the software CAS. If two vehicles arrived simultaneously in blocks B1 and B2, the hardware could command S1 and S2 on at the same time. However, the safe tone CAS, by its discrete nature, cannot have a corresponding failure. The discrete software logic term cannot assume both the value "1" and "0" at the same time. Therefore, even if the hardware CAS fails in this manner, the software CAS will function correctly, and a disparity will result.

$\overline{B3}$ Fails Low. With this failure, neither S1 or S2 can be turned on. It is a safe failure condition and is detected when the first vehicle to arrive causes a disparity with normal system operation.

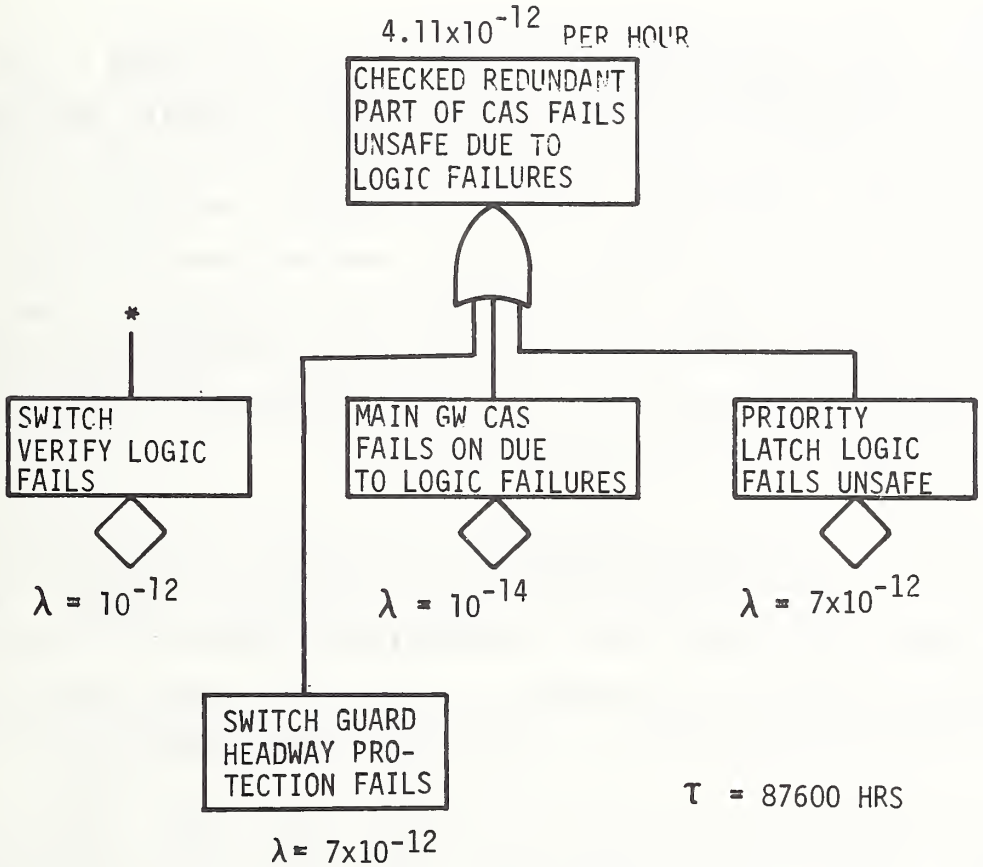
$\overline{B3}$ Fails High. If $\overline{B3}$ fails to "1" (block B3 unoccupied), it is not immediately detectable since it does not cause a change in the output of gate G5. It is also not detected in normal operation when a vehicle negotiates the merge. The expression for S1 is:

$$S1 = B1 \bullet Q \bullet \overline{B3} \text{ (safe tone ON).}$$

The safe tone S1 is turned on when block B1 becomes occupied. In normal operation, block B3 is then unoccupied ($\overline{B3} = 1$); the fact that $\overline{B3}$ has failed to "1" has no immediate effect and, therefore, is not detected. This failure is not detected until a vehicle enters block B1 while Block B3 is occupied. When this happens, the failed hardware CAS will set S1 to "1" (safe tone on) but the unfailed software CAS will not command the safe tone on, and a disparity will result. A vehicle entering

block B1 with block B3 occupied is an abnormal event, and the interval between such events may be months or years. This provides a large time window for the corresponding failure to occur in the software CAS. If this happens, safe tone S1 will be turned on and the vehicle in block B3 will be unprotected. The time window is limited by special monthly tests. The original Bendix study analysis of this fault scenario includes a detailed Failure Modes & Effects Analysis (FMEA). The results show that the probability of occurrence of an unsafe condition is 7×10^{-12} per hour.

5.1.1.1.4 Checked Redundant CAS Fault Tree. Figure 5-5 summarizes the analysis of logic failures in the checked redundant part of the CAS.


4.11x10^-12 PER HOUR
CHECKED REDUNDANT PART OF CAS FAILS UNSAFE DUE TO LOGIC FAILURES
*
SWITCH VERIFY LOGIC FAILS
λ = 10^-12
MAIN GW CAS FAILS ON DUE TO LOGIC FAILURES
λ = 10^-14
PRIORITY LATCH LOGIC FAILS UNSAFE
λ = 7x10^-12
SWITCH GUARD HEADWAY PRO-TECTION FAILS
λ = 7x10^-12
τ = 87600 HRS

*Note: Although analyzed together with other CAS logic, this item is not relevent to avoidance of collisions between vehicles and is, therefore, not included numerically. (See Section 5.1.1.)

FIGURE 5-5. CHECKED REDUNDANCY FAULT TREE

Where necessary, the failure rates have been converted to "per unit per hour". The predominant contributors are loss of headway protection in the switch guard and merge guard circuitry. These failures are discussed above. The Bendix study analysis shows the probability of these failures to be 7×10^{-12} per hour which is similar to that claimed for fail-safe devices employed in the railroad industry (i.e., 10^{-12}). It should be pointed out that for simplicity this analysis assumes that all failures on the fault tree last for ten years. This is conservative in that some modes of failure may be detected before this time. The realistic failure rate of the checked portion of the CAS is probably at least one order of magnitude smaller than that estimated here. This fault tree is used in determining the overall safety of the CAS in Section 5.1.1.

5.1.1.2 Fail-safe Circuits. Fail-safe circuits are those circuits which are used single thread (i.e., not subject to checked redundancy) and which could have a safety impact if the circuit were not fail-safe. These circuits include the switch verify receiver, the loop driver, the control gate, the disparity detector, and the disparity latch. The Bendix safety study included detailed circuit analyses of each of these, and the results are summarized in the following paragraphs. Paragraph 5.1.1.2.6 presents a fault tree quantifying the impact of unsafe failure in the single thread circuits.

5.1.1.2.1 Switch Verify Receiver. The switch verification receiver amplifies, filters, and detects an amplitude-modulated carrier. Two narrow band filters select the 50-Hz modulation components. The filter outputs are combined and converted to a 50-or-70 Hz square wave and transferred to the CAS logic for additional signal processing.

Failure of the receiver to react to a normal input signal from a vehicle is safe. Failure of the output high or low is safe. In both instances the CAS logic will not receive a switch verification signal, and the safe tone will not be turned on.

The only potentially unsafe failure mode is a failed condition whereby the receiver goes into oscillation and its output simulates the square

wave of a switch verification signal. A threshold of 0.52 amplitude is required to switch verify. The Bendix analysis estimates that the probability of a failure mode causing self-oscillation and resulting in a signal greater than the 0.5v threshold is 6×10^{-10} per system hour. In addition, for a hazardous situation to result, this false switch verification signal must occur when the corresponding block is occupied or within three seconds of its becoming occupied; otherwise the software CAS will create a disparity. (See Section 5.1.1.1.2, Switch Verification Logic Fails Low.) The improbability of the failure occurrence in the first place coupled with the fact that it must occur in a specific 3-second time window makes the probability of a hazardous situation far smaller than the previously quoted failure rate for circuit failure alone.

5.1.1.2.2 Loop Driver. The loop driver supplies a 10.2 kHz carrier signal which is then modulated at a 50-Hz rate to signify safe tone on. When the 50-Hz modulation is absent, the safe tone is off and no signal is supplied to the safe tone loops. One driver normally feeds four loops.

The loop driver circuitry is inherently fail-safe as far as single failures are concerned. Failure of the carrier OFF, or of the 50-Hz modulation continuously high or continuously low, are all safe since the safe tone loop must be supplied both the 10.2 kHz carrier and the 50-Hz modulation signals to be interpreted as ON by a vehicle. Two potentially unsafe failure modes, both of which require at least two failures, have been identified. These are discussed below.

50-Hz Modulation Reflection. One constant voltage 10.2-kHz carrier source is connected to four loops and each loop is turned on and off by a transistor switch controlled by 50-Hz modulation, as shown in Figure 5-6a (where only two loops are shown instead of the usual four). Failure of the switching transistor in the on or off condition is a safe failure. But if the loop driver develops an internal resistance and a transistor switch fails, 50-Hz modulation can be reflected from the adjacent loop making the first loop appear on when it should beoff. This phenomenon is known as "common impedence coupling."

Referring to Figure 5-6 during the half cycle that the switch is off:

$$I_{1off} = \frac{V_i}{R_s + 60} \quad ;$$

and during the half cycle that the switch is on:

$$I_{1on} = 1/2 \quad \frac{V_i}{R + 30} \quad .$$

The ratio of $I_{1\ off}$ to $I_{1\ on}$ is:

$$\frac{I_{1off}}{I_{2off}} = 2 \quad \frac{R_s + 30}{R_s + 60} \quad .$$

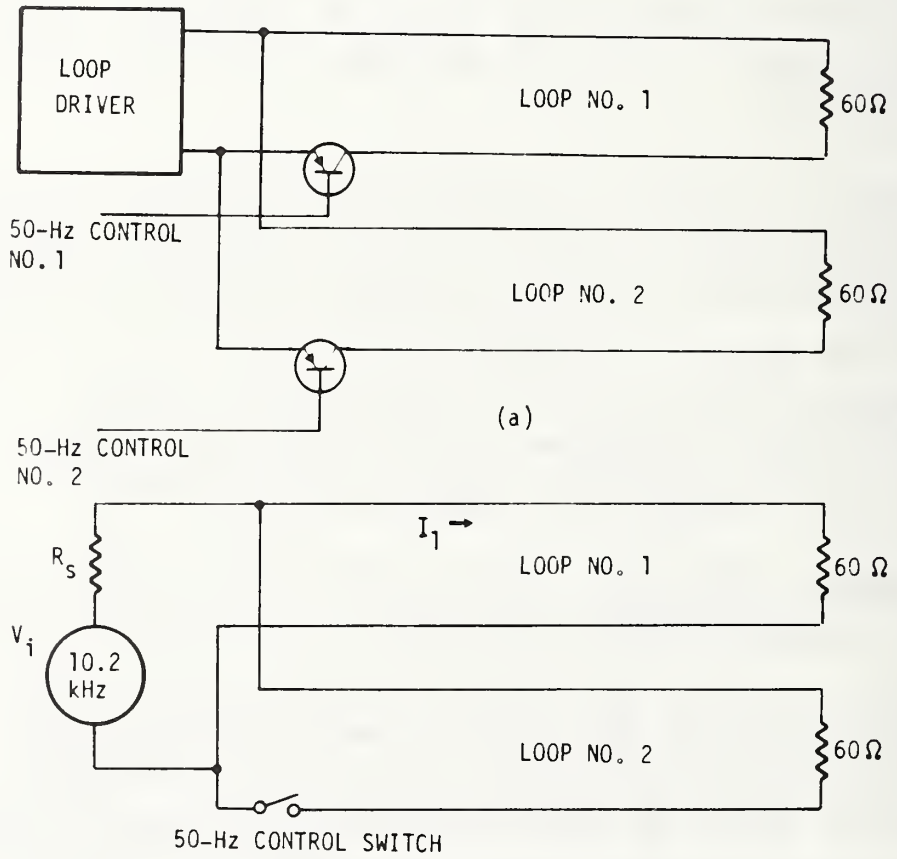


FIGURE 5-6 LOOP DRIVER

If R_s is small, as is normal for a constant voltage driver, no 50 Hz will be coupled into loop No. 1. As R_s fails to a high value, this ratio approaches 2 and coupling from loop No. 1 to loop No. 2 occurs. It should be noted that the current in both loops would be much reduced below normal in this failure mode, but depending on vehicle thresholds and margins and the value of R_s, 10.2 kHz modulated at 50 Hz could be seen by a vehicle over loop No. 1 because loop No. 2 is on.

The failure mode is the combination of a shorted or saturated modulation transistor and a high source impedance. The Bendix analysis identified the individual component failures that can produce this failure mode and estimates the probability of occurrence to be 1.2×10^{-13} per system hour.

Loop Driver Oscillation. A hazard of such a nature as to produce a false signal corresponding to a safe tone on potentially exists if oscillation occurs in any loop driver. The probability of oscillation of this nature due to component failure is low since both carrier frequency and modulation must occur. The 50-Hz modulation transistor must be circumvented to provide current to the loop. The frequencies must be sufficiently close to the design values and of sufficient amplitude to be accepted by the vehicle. The Bendix study estimates the probability of this failure mode to be 3×10^{-10} per system hour.

5.1.1.2.3 Control Gate. The control gate performs the function of passing the 50-Hz safe tone frequency to the loop driver modulator, or of stopping the 50-Hz as specified by the safe tone control signal. The safe tone control signal is part of the checked redundant CAS, but subsequent electronics, (i.e., the control gate and loop driver) are not checked and must be fail-safe.

A schematic of the control gate is shown in Figure 5-7. Part of the gate is on the disparity detector board and part on the loop driver board, as shown. The safe tone control signal input is 0 volts = off and open circuit = on. That is, when Point A is at 0 volts, there should be no failure which can allow the 50-Hz signal on the base of Q2 to get onto the base of Q3. In normal operaion, when A = 0 volts,

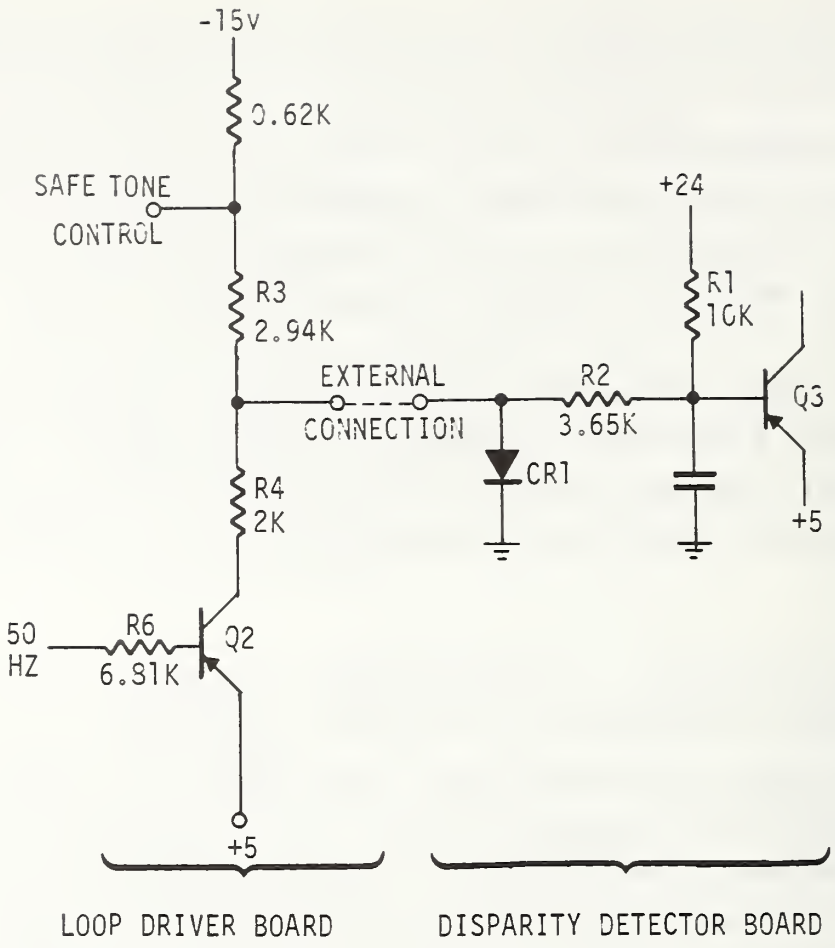


FIGURE 5-7. CONTROL GATE

the 50-Hz signal on the collector of Q2 is shunted to ground via CR1. When A is open, Q3 is biased "on" when Q2 is not conducting, and "off" when Q2 is conducting. Q2 operates continuously at a 50-Hz rate.

The Bendix analysis identifies only one failure mode which, in itself, is not fail-safe but explains why this cannot happen. If CR1 opens, the fault would be undetected except through routine maintenance. However, Q3 will not switch unless the +24V supply voltage also drops. If the +24V supply drops sufficiently, Q3 is turned on and off by the 50-Hz modulation signal. The magnitude of the +24V supply required to cause this unsafe condition is 10.82 volts. If the +24V supply decreases enough further, Q3 would remain on continuously, which is a safe condition. The magnitude of the +24V supply which would hold Q3 on, is +7.03 volts. Thus, an unsafe condition could occur if the +24V supply decreases to between +10.82 and +7.03V.

Since there is only one +24 volt supply per station, if the power supply output drops, it will affect all cards. However, +24 volts is monitored in the Disparity Latch circuit, and the 50-Hz source will be latched off if +24V drops below a predetermined level. The worst case lowest level to insure that the 50-Hz is latched off is 19.76v. This is well above the +11.6V at which an unsafe condition could occur in the Control Gate. Thus, failure of the +24 volt supply is safe.

5.1.1.2.4 Disparity Detector. A schematic of the disparity detector is shown in Figure 5-8. The 50-Hz ac tracer is applied to one input of an operational amplifier at reduced amplitude and offset from ground. If the other input to the operational amplifier is held at a bias equal to the bias on the 50-Hz input, the output of the amplifier will be 50-Hz at an amplitude of ± its output saturation voltage.

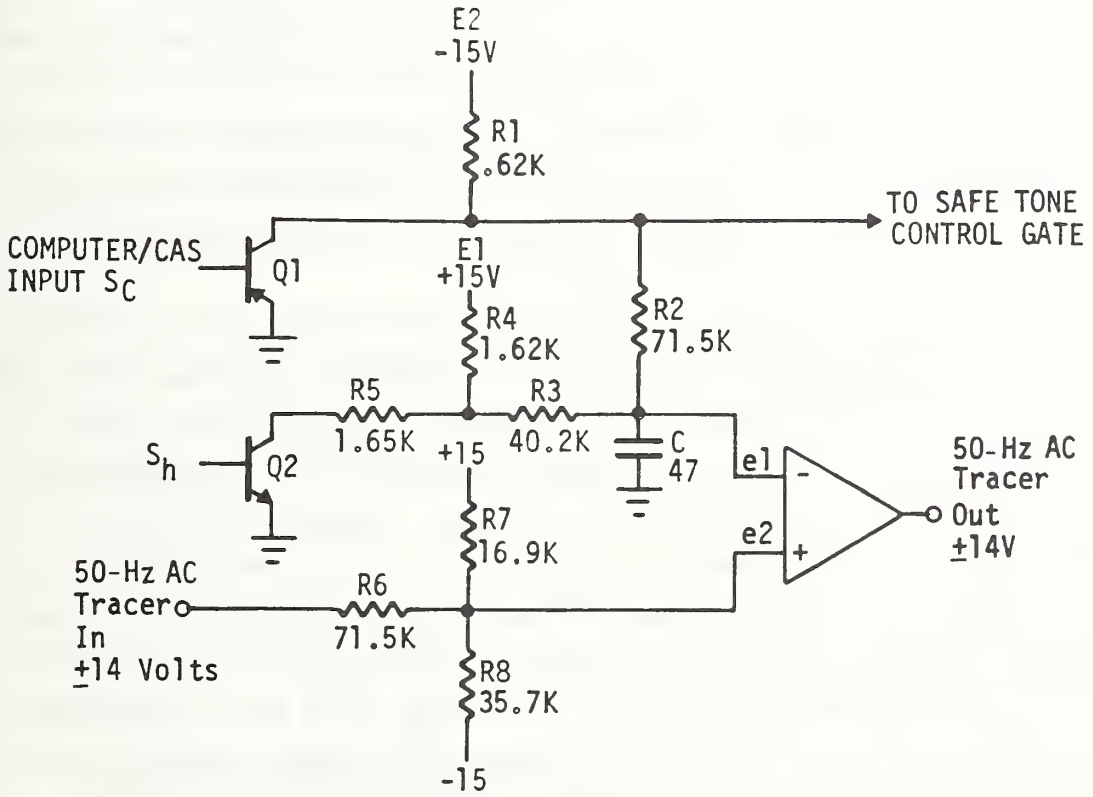


FIGURE 5-8. DISPARITY DETECTOR

If the two logic signals, one from the computer/CAS and the other from the hardware logic, "agree", the bias e1 will be of a value which enables the tracer to pass through the amplifier. If the two logic signals

disagree, the amplifier will be biased to slew to one of its saturation voltages, and no ac tracer signal will pass.

The Bendix study contains a circuit failure analysis which, with one exception, shows the disparity detector to be fail-safe provided certain resistors do not fail shorted. Employed in this circuit is a particular type of resistor (RNR), which may increase resistance slightly (0.125 percent in 4.5 years) or can fail open, but which is manufactured in such a manner as not to fail shorted. This is supported by available reliability data, and these resistors are claimed to be comparable (as far as failing shorted is concerned) to fail-safe devices used historically on railroads which have (unsafe) failure rates on the order of 10^{-12} per unit per hour.

If resistor R6 failed shorted, the amplitude of the 50-Hz signal into the amplifier, e2, would increase sufficiently that the amplifier would pass the signal even when the bias level, e1, was such that the 50-Hz should be inhibited. Assuming that the amplifier did not burn out or otherwise fail, this would constitute an undetected single point failure. Therefore, resistors that do not fail shorted are used.

The exception to fail-safe operation mentioned previously involves failure of both transistors, Q1 and Q2. Normally a guideway safe tone is on, the two CAS signals are in agreement, and the 50-Hz signal is passed by the amplifier. If either transistor fails in such a manner that its output signal level cannot change, immediate detection will not occur since the transistor has failed in the state that it was currently in (i.e. it's output did not change). So far this is safe. When a vehicle passes and the safe tone should go off, the computer CAS and the hardware CAS signals, Sc and Sh, will be in disagreement, and a disparity will result. If, however, the other transistor fails in a similar manner before the first failure is detected by the passing of a vehicle, both the hardware and computer CAS have effectively failed in the same unsafe state. The safe tone will not turn off, and the failure will not be detected.

The above failure mode requires two independent failures but is unsafe, and the probability of occurrence must be determined. Typical failure rates (λ) for the transistors are 10^{-8} per hour. A conservative assumption is that a vehicle does not pass for 10 hours (τ) after the first failure has occurred.

Using $\lambda-\tau$ Method:

Prob. of first failure = 2×10^{-8} per hour (either transistor);

prob. of second failure within 10 hours after first = $10^{-8} \times 10$;

prob. of both = $2 \times 10^{-8} \times 10^{-8} \times 10$ per hour
= 2×10^{-15} per hour.

Thus, the probability of undetected, unsafe failure is negligible.

5.1.1.2.5 Disparity Latch. A Disparity Latch schematic is shown in Figure 5-9. The 50- Hz TTL signal is converted to a 50-Hz high level tracer signal by amplifier A1.

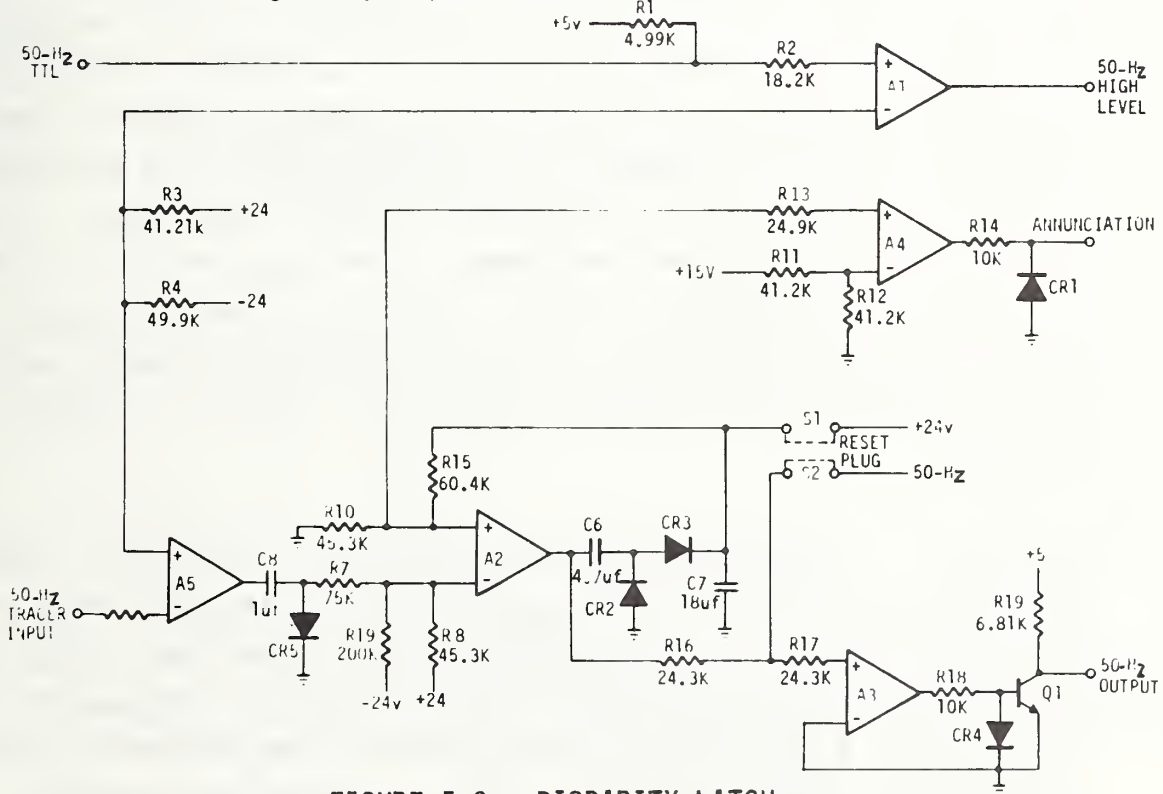


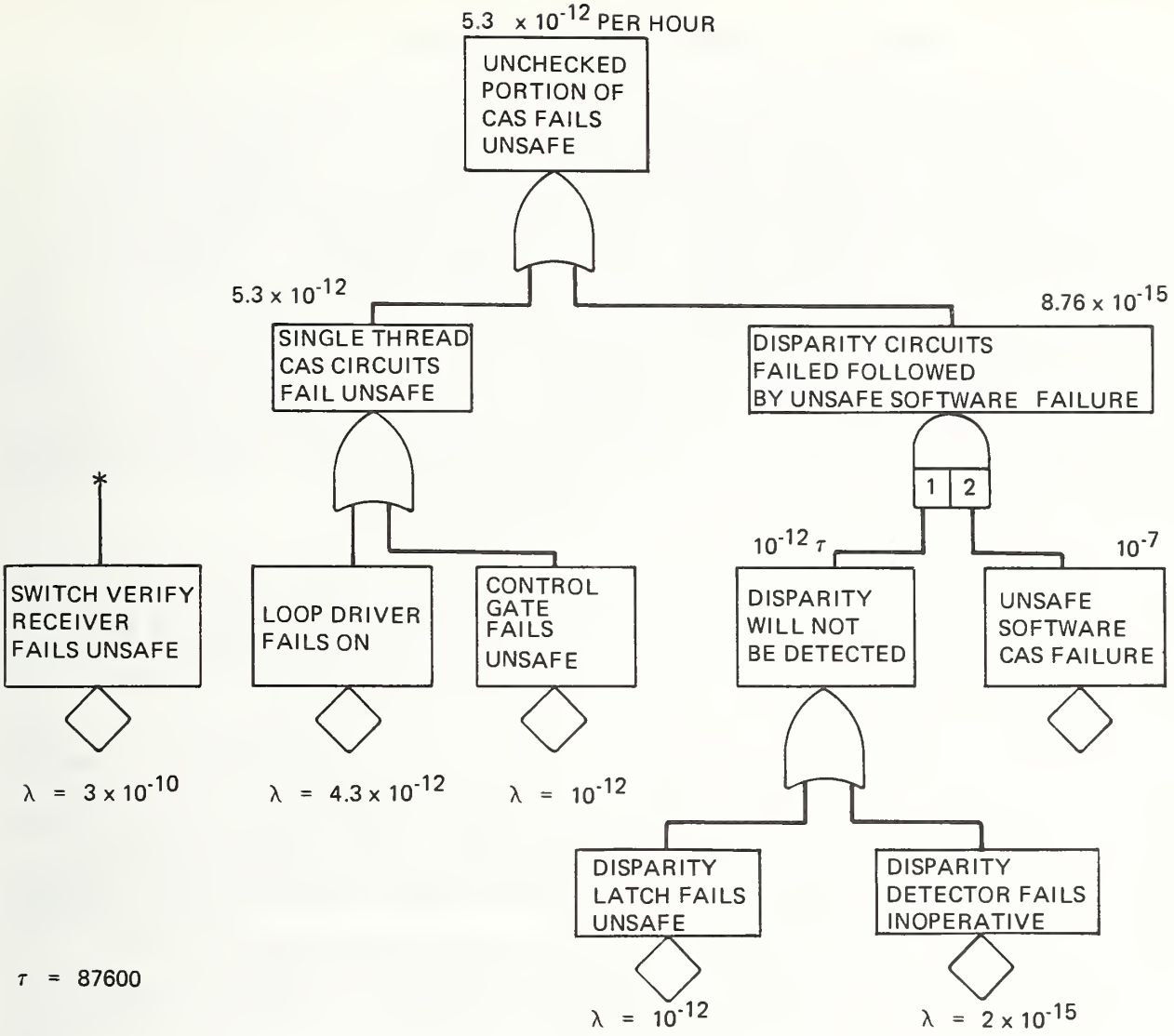
FIGURE 5-9. DISPARITY LATCH

This amplifier also monitors +24 and -24 volt power supplies. The high level signal feeds the first of the string of disparity detectors. The output of the last disparity detector enters the board at "tracer in". Amplifier A2 provides the latching function. As long as there is a 50-Hz signal out of A2, the diode network provides a positive feedback bias to keep A2 on. If the signal at the + input of A2 drops (or rises), the ac output from A2 stops and remains off until the bias signal is reset.

Amplifier A3 provides 50-Hz to all control gates. Obviously, if there is no signal from A2, there is no 50-Hz signal from A3. Amplifier A4 provides a dc annunciation signal to indicate the status of the latch. Switches S1 and S2 are used to reset (override) the latch if a disparity occurs.

The disparity latch circuit is inherently fail-safe by the nature of its design. The active output is a 50-Hz square wave. The Bendix analysis shows how any component failures, with one exception, will cause a continuously high or continuously low output but cannot erroneously pass the 50-Hz signal. If S1 and S2 (depicted as switches in Figure 5-9) fail closed the latch will be inadvertently overriden and 60-Hz will be passed to the CAS control gates. In actuality, S1 and S2 physically consist of a single "override plug" which is manually inserted when required. As such, it cannot fail in itself, but it could be inserted at the wrong time or inadvertantly left in due to human error. In the Morgantown system, this contingency is strictly controlled by procedural means. The procedure requires a dialogue between the central operators and the maintenance person in the station equipment room, and the logging of the override plugs "in" and "out" by the central operator.

5.1.1.2.6 Unchecked CAS Circuits Fault Tree. Figure 5-10 summarizes the analysis of failures in the unchecked part of the CAS. Where necessary, the failure rates have been converted to per unit per hour. Since the safe tones are controlled by the software CAS with the possibility of inhibit by a disparity, this branch requires two independent failures to be unsafe. The loop driver and the control gate are completely single-thread and are the dominant contributor to unsafe failure of



*Note: Although analyzed together with other CAS circuits, this item is not relevant to avoidance of collisions between vehicles and is, therefore, not included numerically. (See Section 5.1.1.)

FIGURE 5-10. NON-CHECKED FAULT TREE

the unchecked portion of the CAS. In any design concept there must eventually be some element that is single-thread, irrespective of the amount of checking performed or redundancy up-stream of the final element. In this case, the dominant failure rate is 5.3 X 10^{-12} per hour. It should be pointed out that, for simplicity, this analysis assumes that all failures on the fault tree last for ten years (i.e., no repair). This is conservative in that some modes of failure may be detected before this time. The realistic failure rate of the unchecked CAS is probably at least one order of magnitude smaller than that estimated here. This fault tree is used in determining the overall safety of the CAS in Section 5.1.1.

5.1.2 Problems Encountered and Their Solution

The initial CAS design presented certain areas of concern in which either the purpose of the CAS could have been defeated or inadequate stopping margins could have resulted. Two of these areas were "vehicle slide-through" and guideway merges. Vehicle slide-through is an anomalous condition in which two vehicles occupy the same block. When the first vehicle departs, the safe tone is turned on in the previous block leaving the second vehicle with no rear protection. This concern was resolved by modifying the software so that the previous safe tone is not turned back on when a vehicle enters a block already occupied.

In the early design safe tones were normally on in merge areas. Two vehicles arriving simultaneously could cause a "lock-up" whereby both vehicles would be stopped, requiring manual operation to clear the problem. Additionally, if one vehicle were "silent", due to other failures, a collision could result. This concern was resolved by inverting the safe tone concept so that safe tones in merge areas are normally off and turned on only when a vehicle arrives. The lock-up situation is avoided by the introduction of priority logic which allows one vehicle to continue through the merge. A more detailed description of the above two areas of concern is provided in Section 4.1 Design Concept.

The following areas of concern involved hardware considerations. Shorts between adjacent conductors on CAS logic cards could cause safe tones to be on when they should be off. This problem was eliminated by redesigning the board layout. Shorts between adjacent pins on drawer connectors could circumvent safe tone control circuits by causing self-oscillation of a switch tone receiver or by effectively paralleling two PDs, thereby eliminating redundancy. These problems were resolved by the use of heat-shrink tubing on drawer connector wiring. Inadequate stopping margins could result due to similar, but not identical, CAS logic cards installed in a wrong location. This possibility was eliminated by physical "keying" so that a card cannot be inserted in an erroneous location. The same problem and solution applied to the speed tone cards which govern vehicle speed on different sections of the guideway.

The initial CAS design employed a master reset toggle switch on each CAS logic equipment rack to clear block occupancy logic station-wide. The switch was not keyed in any way. It could be inadvertantly or inappropriately activated and was the source of a single point failure that would clear the logic. This switch has been retained out of necessity for servicing the hardware CAS. However, it is a lock type, spring loaded switch. The safety concern relative to this switch was automatically dispelled when the dual hardware/software CAS concept was introduced since inadvertant activation or unsafe failure will now cause a CAS disparity. This subject is recounted here as a typical example of a system function which contains potentially hazardous overtones. It should only be implemented if absolutely required, and then the potential hazard must be negated by other means, as is the case here.

5.2 CAS TESTING

The CAS components were tested using normal component level testing. All components were verified to provide expected outputs in response to all inputs.

Integration testing was exceptionally thorough. The CAS logic was exhaustively tested at multiple subsystem levels. First, the software CAS and the firmware CAS were separately checked out. Next, they were tested in a system integration laboratory (SIL). After installation at Morgantown each station CAS was tested. Finally, the complete system was tested using the same exhaustive test scenarios used for the lower level tests.

Individual safe tones were also thoroughly tested to verify that each safe tone loop was adequately isolated from all other safe tone loops.

The following sections describe the CAS logic and safe tone loop testing. Component level testing is not discussed since the component tests were similar to tests performed on non-CAS components.

5.2.1 Test Scenarios

Test scenarios were developed to verify that the CAS equations were properly implemented. Three types of scenarios were developed. The first type tests normal operation by simulating a vehicle trip over all possible paths.

The second type is a backwards scenario that simulates a vehicle traveling backwards over all possible paths. This is done twice without a reset in between. The first trip leaves all blocks occupied. This occurs because each block's arrival PD is hit after the block's departure PD. Thus, each block is set occupied but is not cleared. At the end of this trip all safe tones are off, and all blocks are occupied. The second trip creates a block occupancy sequence which is the inverse of that for forward movement (i.e., each step clears one occupied block and sets the previous clear block occupied). At each step all blocks except the single clear block are occupied. This verifies that:

1. no safetone equation contains unnecessary "block clear" terms;

2. a clear block will not turn on safe tones which should not be dependent upon the block. (This is primarily of interest for the hardwired logic in which "block clear" is an active signal.)

The third type of scenario verifies that all terms in the CAS equation not checked by the above two types are present in the equations. These scenarios represent anomalous conditions; hence they do not necessarily follow realizable vehicle trajectories.

5.2.2 System Integration Laboratory Tests

Before the CAS equipment was installed in Morgantown, the components were integrated and tested in a System Integration Laboratory (SIL).

First, the software CAS was exhaustively tested using a version of the software CAS modified to read PD and switch latch inputs specified by the scenarios described above. Safe tone status was recorded and compared with the expected results using automatic file compare software.

Then the firmware was totally tested using a special configuration to read scenario inputs and record results. The firmware was not commited to read-only-memory (ROM) until the stand alone testing was completed. Instead, read/write memory (RAM) was used to simplify correction of errors.

After the software and hardware CAS had been separately verified, integration testing was performed on the CAS equipment shown in Figure 5-11.

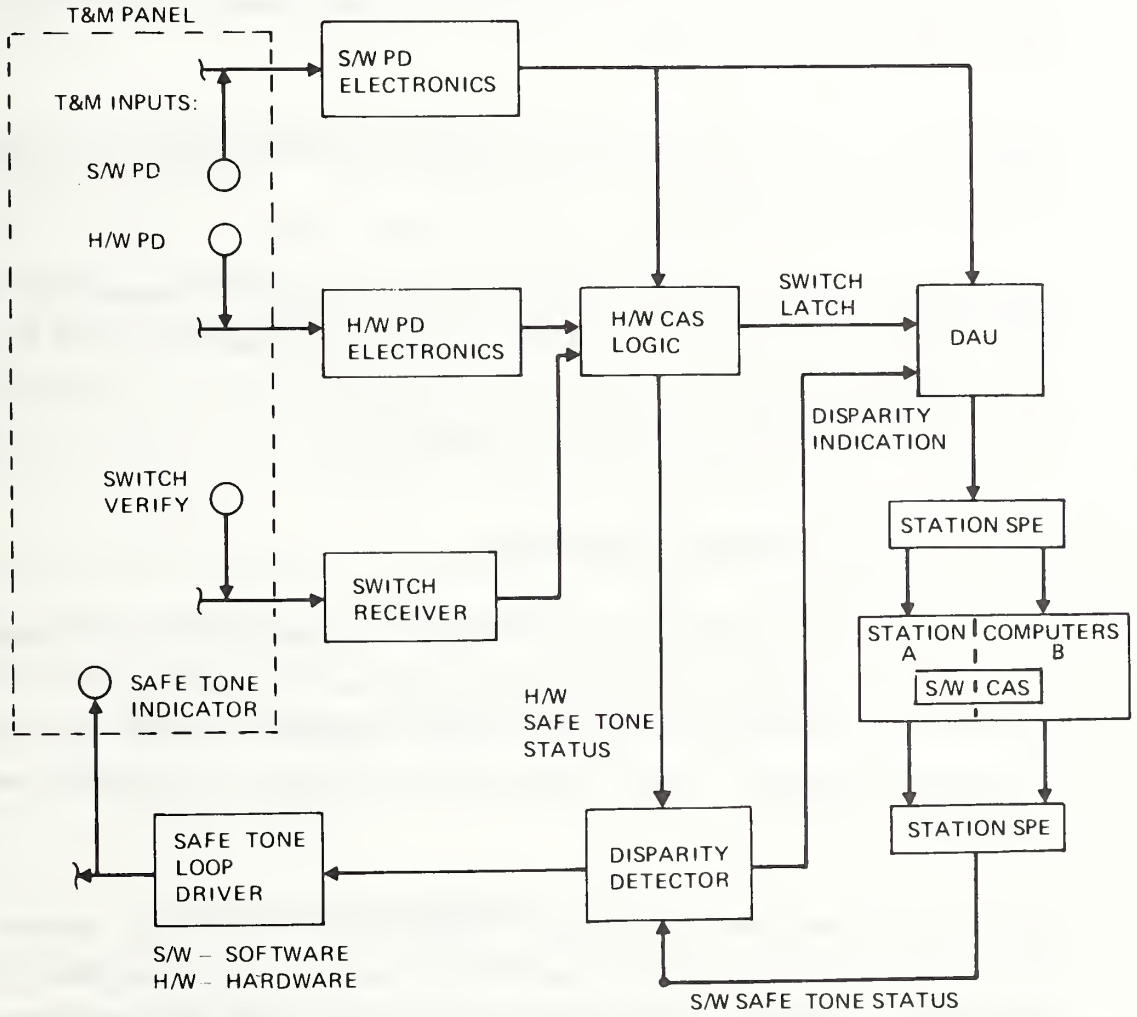


FIGURE 5-11. CAS EQUIPMENT TESTED AT SIL

The integration testing was performed using the Test and Maintenance (T&M) panel to provide PD activation and switch verification. Results were monitored by observing safe tone LED indicators on the T&M panel and disparity LED indicators on the CAS equipment drawer. The following objectives were met.

Objective 1. Verify that one for one correspondence exists between simulated PDs and T&M Panel PD switches and that panel switches are labeled correctly.

Objective 2. Verify that one for one correspondence exists between T&M Panel LEDs and guideway safe tone loops and that the LEDs are labeled correctly.

Objective 3. Verify correct operation of the disparity LED display and disparity override plug.

Objective 4. Verify that the CAS controls the safe tones in accordance with the logic equations.

Objective 5. Verify that a disparity that exists for between 0.5 second and 1 second will result in a safe tone being turned off within 1 second after disparity onset. Verify that disparities can be initiated by activation of any software PD or hardware PD.

5.2.3 Logic Tests at Morgantown

The CAS for each station was tested following installation at Morgantown. This testing essentially repeated the previous SIL testing, the only difference being the use of installed CAS equipment and the inclusion of guideway equipment - PDs, safe tones, and switch verification were connected.

After the CAS had been successfully tested at all stations, system testing was performed on the complete CAS using a full complement of operational software. All testing to this point had been performed

using the CAS software which was modified to allow operation under control of a special Input/Output Test Program (IOT). IOT was designed to support checkout of station equipment using the station computer without operation of the central computer. The CAS software used with IOT was modified to eliminate the following functions which could not be supported by IOT:

1. Automatic Reset,

2. Slide-through protection at handover,

3. Detection of false switch verification.

The interface with IOT also differed from that with the operational software.

The above modifications were minor and did not affect the primary function of the software CAS - safe tone control. The three omitted functions were verified by formal Product Assurance testing of the operational software. This approach was successful as the software CAS was error free when the system test was performed.

The system test was conducted to verify the correct operation of the Phase II CAS as implemented by operational hardware and software.

Using the CAS T&M panel to execute scenarios simulating vehicle movement, CAS logic operation at each station was verified for:

a. normal guideway travel in both directions,

b. ramp movements,

c. station channel movement,

d. conflicts,

e. switch verification.

Disparity detection and reporting was verified for items a, b, and c. Slide through protection at all handover points and software reaction to false switch verification were also verified.

Test Objectives/Success Criteria

Objective 1 - Trailing Vehicle

Verify that the CAS provides trailing vehicle collision avoidance protection.

PD activation removes safe tone signal from the first safe tone loop trailing the activated PD and restores safe tone signal to the second safe tone loop trailing the activated PD.

Objective 2 - Merge Protection

Verify that the CAS provides collision avoidance protection at all merge points.

For the priority channel at merges, the normally "off" safe tone in that channel is turned "on", and the safe tone in the other channel remains "off."

Objective 3 - Switch Procedure

Verify that the CAS provides collision avoidance protection at all switch points.

At switch regions, normally "off" safe tones remain "off" in the event a switch verification is not received.

Objective 4 - Disparity Detection

Verify that near simultaneous activation of the dual PDs is required for correct operation of the CAS logic.

Upon activation of only one of the dual PDs (H/W or S/W), a disparity is detected and the safe tone signal is removed from all safetone loops in that CAS zone.

Objective 5 - Slidethrough at Handover

Verify that the same slide-through protection exists at handover points as does on the rest of the guideway.

The vehicle remaining in a previously dual-occupied block is protected by an "off" safe tone loop behind it.

Note: After slide-through, two vehicles occupy the same block. Subsequently, one of the vehicles moves forward.

5.2.4 Safe Tone Feedthrough Tests

The safe tone feedthrough tests were conducted to verify that the level of each safe tone was within acceptable limits for ON and for OFF status:

ON	OFF
6 to 34 (MV P-P) at 1-1/2 inches	0.25 (MV P-P) at 1-7/8 inches

The safe tone ON level was verified with all safe tones OFF except the safe tone under test. Safe tone OFF level was verified with all safe tones ON except the safe tones under test.

Tests were also conducted to verify that each switch verification loop was performing properly (i.e., that a switch verify would be produced if a proper verification signal was provided - otherwise not).

6. POTENTIAL IMPROVEMENTS

The current CAS design evolved through three phases of development. At each juncture various alternatives were considered and the best solution was selected. No changes have been identified to improve the performance of the MPM CAS. However, certain design alternatives should be reconsidered before a CAS is installed in a future system. The following discussion examines two types of changes - alternatives to specific MPM design choices and changes which would be required to extend the CAS capabilities to meet new guideway traffic requirements.

6.1 DESIGN ALTERNATIVES

The current CAS design reflects design choices based upon MPM requirements. Whenever new requirements were recognized, the simplest satisfactory solution was selected. The following alternatives are presented since altered circumstances might lead to different choices.

6.1.1 Checked Redundancy Alternatives

The initial design proposed for the dual CAS treated the hardware and software CAS equally. Safe tone commands from the two systems were to be combined by an AND gate to control the safe tones. This was in addition to the disparity checking used in the current system. Thus, a disparity would doubly remove the safe tone. A disparity occurs only if one input is "0" (the other is "1"); hence, the AND gate output is "0". The disparity would also remove the 50-Hz tracer as in the current design.

Safety analysis showed that double reaction to a disparity was not necessary. System shut down is sufficient; hence, the AND gate was not implemented. This reduced cost and system complexity as shown in Figure 6-1.

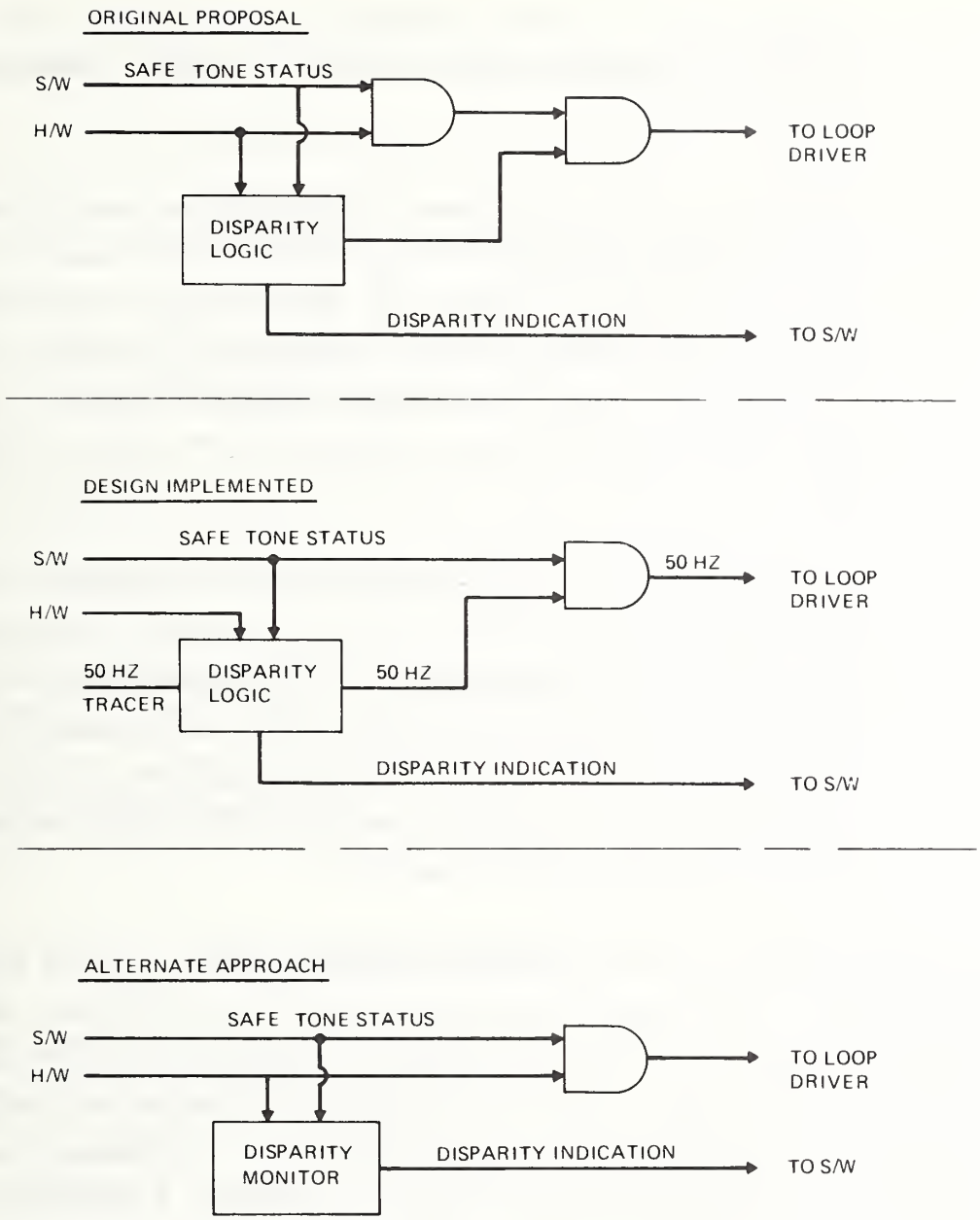


FIGURE 6-1. DUAL CAS ALTERNATIVES

An alternative approach, also shown in Figure 6-1, would AND the hardware and software safe tone commands and rely upon software action to provide system shutdown if a disparity occurs. Conceptually, this approach provides adequate safety since the disparate safe tone is off and the opportunity for the second failure is limited to the time required to stop approaching vehicles. If safety requirements can be satisfied, this approach looks attractive for three reasons.

1. Passenger comfort would be improved since vehicles would be stopped by normal brakes (2 ft/s^2) instead of emergency brakes (10 ft/s^2).

2. Operability could be improved by allowing increased tolerance to transcient disparities. The current system requires shutdown within one second to prevent the possibility of a collision situation developing while the software CAS erroneously keeps a safe tone on. With the proposed approach immediate shutdown would not be required since a disparate safe tone is always off.

3. The possibility of increased tolerance to transient disparities might reopen the possibility of using continuous detection for one CAS leg. One objection to continuous detection has been the likelihood that timing problems would make the system inoperable. (Detection of block occupancy changes would be hard to synchronize due to response differences between discrete and continuous detection.)

A serious drawback to the alternative approach is the need for a fail-safe AND gate. The hardware and software safe tone status must be combined by a device which does not have an "always on" failure mode. The current system uses a fail-safe technique to combine the software and disparity detector votes. The technique used is dependent upon the 50-Hz output provided by the disparity detector. A comparable approach may not be feasible to "AND" the hardware and software votes.

6.1.2 Firmware CAS

The firmware CAS, implemented in the Phase II stations, is similar to and more economical than the hardwired CAS logic used in the Phase I stations. In addition to simplicity and economy the firmware CAS offers the following potential advantages.

1. Enhanced capabilities are possible:

    a. Advanced reset capability,
    b. CAS testing,
    c. Simplified Slide-through protection. (See Section 6.1.3.)

2. Failure Modes unique to hardware are eliminated (e.g., contradictory priority latch status).

Both systems are very reliable. The firmware CAS is believed to offer a reliability advantage for large applications. However, neither system has experienced enough failures at Morgantown to indicate any difference.

A dual firmware CAS should be considered as an alternative to the current software/hardware CAS. This would reduce CAS dependence upon the control computer. If this approach is used, the two microprocessors should be programmed independently as are the current software and firmware CAS.

6.1.3 Slide-Through Protection

The decision to provide slide-through protection per the current design was influenced by the simplicity of the resulting hardwired logic. In the hardwired logic a block is cleared by a pulse which occurs when the status of the block ahead changes from unoccupied to occupied. Thus, slide-through protection was provided without increasing the complexity of the hardwired CAS logic. This was clearly the best choice for a hardwired CAS. However, this may not be the best approach for a software or firmware CAS. An alternative approach would replace check-in/check-out logic with count-in/count-out logic. Block occupancy would be incremented by activation of the block entrance PD and decremented (if positive) by activation of the exit PD. Thus, block status would contain a vehicle count which would not be cleared by departure of the lead vehicle following a slide-through. This approach is straightforward, is slightly simpler to program, and offers two advantages.

1. Slide-through protection can be provided at handover locations without requiring block occupancy communication between stations.

2. Slide-through recovery would be simplified. No CAS reset would be required. (The current design requires a CAS reset after the lead vehicle departs. Otherwise the trailing block would remain occupied after both vehicles have departed.)

The second advantage is hypothetical since slide-through is very improbable.

One drawback to count-in/count-out logic is the effect of multiple PD activation. Multiple activation of a PD will not adversly affect check-in/check-out operation since a block is either occupied or clear. Count-in/count-out logic would be adversely affected since the count would be erroneous. False counts can be filtered, but the increased complexity may not be justified. This alternative should only be considered for a system in which multiple activation is rare.

6.1.4 Switch Verification

There is some question regarding the need for switch failure protection. Safety anlaysis of improved steering systems may conclude that switch guard logic can be eliminated. If switch guard logic is included in a future system, the following improvements should be considered.

1. Upon detection of a false switch verify signal, it should be sufficient for the software CAS to hold the switch guard off (as does the hardware CAS) and stop approaching vehicles by normal brake commands. This would be done in lieu of creating a disparity as done in the current system.

2. The PD before a switch guard need not clear the switch latch. The latch is cleared by switch guard exit PDs. If an exit PD is not activated the next vehicle cannot reach the switch guard because the previous safe tone remains off.

3. The software switch latch should be computed by the software. Reset capability (comparable to that for the hardware CAS) could then be added at minimal cost.

6.1.5 Merge Control

If a conflict between a vehicle departing a station and vehicles on the main guideway is probable, the control software is required to stop the departing vehicle before merge priority is granted to the departure ramp. If this were not done, the resulting merge conflict would stop vehicles on the main guideway. The current CAS layout grants priority at merge entry (i.e., when a vehicle enters the block before the merge guard block). This allows the merge guard to be turned on before the vehicle arrives.

The merge conflict check must occur when a vehicle enters the block before merge entry (i.e., two blocks before the merge guard). When a vehicle is dispatched from a position only one block from merge entry, the conflict check must be performed before the vehicle's progress can be meaningfully assessed.

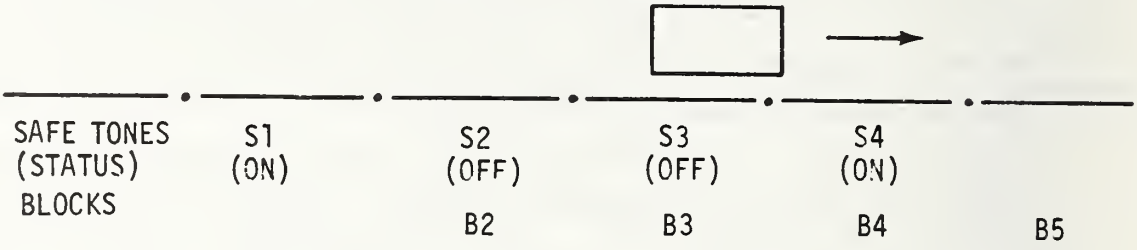
One solution is to use a split safe tone for the merge guard. The first part does not require priority and is just long enough to provide a safe tone until priority is granted and the second part (merge guard safe tone) is turned on. As discussed in Section 4.2.1.4, this approach is currently used where space is limited.

6.2 CAS EXTENSIONS

The MPM CAS concept can be extended to meet future requirements beyond those imposed by the current MPM system. Two such extensions, short headway operation and bidirectional guideway operation, are discussed below.

6.2.1 Short Headway

The MPM system provides for a nominal 15-second headway between vehicles. While this would be considered short headway by most standards, shorter headway is feasible. Headway as short as 7 or 8 seconds appears feasible using multiple block logic illustrated in Figure 6-2.



SAFE TONE EQUATIONS

$S1 = \overline{B2} \cdot \overline{B3}$

$S2 = \overline{B3} \cdot \overline{B4}$

$S3 = \overline{B4} \cdot \overline{B5}$

FIGURE 6-2. TWO-BLOCK CAS

The illustrated logic is called a two-block system because an occupied block removes two trailing safe tones. An n-block system would remove n trailing safe tones. The curent MPM CAS is a single-block system. If block boundaries (i.e., PDs) are aligned with safe tone boundaries, the minimum headway for an n block system is the travel time over n+1 blocks. The minimum block length is the minimal separation (worst case stopping distance plus vehicle length) divided by n. For a constant speed (V) the minimal headway (T) is related to stopping distance (S) by:

$$T = \frac{S}{V}\left(\frac{n+1}{n}\right).$$

The corresponding block length is s/n. For a single block system such as the current MPM CAS, the minimum headway is 2 S/V with a block length of S. For a 2-block system the values are $\frac{3S}{2V}$ and S/2 respectively.

For multiple block system the minimal headway approaches S/V as the number of blocks (n) becomes large. As a practical matter, the headway reduction becomes insufficient to justify the large number of PDs and safe tones required for a multiple block system if the number of blocks gets too large.

For example a 10-block system allows only 10 percent shorter headway than a 5-block system. By contrast, a 2-block system allows 25 percent shorter headway than a single block system.

Examination of Table 4-1 shows that a single-block system will support 10-second headway for MPM vehicles at civil speeds other than 4 ft/s and 44 ft/s. (Table entries corresponding to case 2 do not allow block/safe tone alignment.) Single block logic can also be used in 4 ft/s sections if PDs are offset by a vehicle length. Two-block logic is required to support 10-second headway at 44 ft/s.

Downspeed transitions and transitions between single-and-double block logic require special treatment. In theory both cases can be handled by the layout procedure, illustrated in Figure 4-4, in which PDs are not required to fall on block boundaries. However, this approach is limited to offsets not exceeding a vehicle length. This is because a vehicle stopped by CAS should stop short of the safe tone occupied by the vehicle ahead. Otherwise, special logic would be required to prevent restart of the second vehicle. If this were done via CAS safe tone removal, the lead vehicle would be unable to depart. A short headway (7.5 second) CAS was developed for Phase IA; hence, solutions satisfying all constraints do exist. Allowance for PD offsets up to a vehicle length provides flexibility which simplifies the layout and significantly reduces the number of blocks required in low speed zones.

The number of blocks required can be reduced by reducing the operating margin allowed for vehicle headway variation. MPM operating experience shows that the point follower control system regulates vehicle position much better than originally expected.

This experience indicates the headway operating allowance could be reduced to one second (instead of 2.2) without significant impact to operability.

If the layout constraints were revised as indicated above, a 9-second headway could be supported with a reasobable increase in the number of blocks required for the current 15-second CAS. (The number of blocks would less than double.)

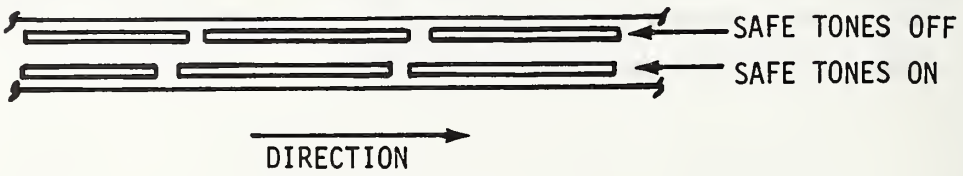
6.2.2 Bidirectional CAS

The MPM CAS is designed for one-way traffic. Safe tones and speed tones are only provided on the right hand side of the guideway and can only be detected on the right side of a vehicle. Thus, a vehicle facing the wrong direction could receive neither speed commands nor a safe tone.

Recent studies have shown that the MPM CAS can be modified to allow two-way travel for special route layouts. These routes provide turn-around capability such that a vehicle could enter a guideway segment for travel in either direction. The vehicles can be essentially identical to MPM vehicles and need only be capable of forward movement. The following paragraphs discuss a fail-safe CAS design and layout supporting such a concept.

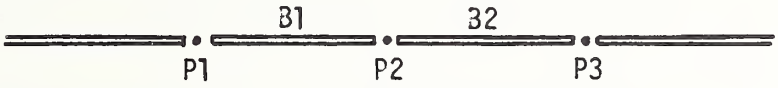
1. One way safe tones

   The safe tone antennas are mounted on the right hand side of vehicles. Safe tone transmission loops are installed on both sides of the guideway but only activated from the side corresponding to the current direction of travel for the particular guideway segment. At a given time only one direction of travel is allowed.

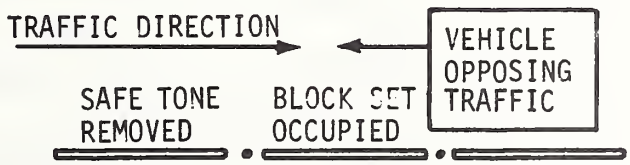


2. Invariant Block Occupancy

The physical guideway assocated with each block is independent of travel direction. Block occupancy can be maintained by a directionally invariant method - when a PD is activated, occupancy status is exchanged between the two blocks adjacent to the PD. In the following example occupancy status is exchanged for B1 and B2 when P2 is activated.



This approach correctly updates block occupancy even if a vehicle moves in the wrong direction. The safety of this approach is illustrated by the following scenario. Assume failure causes a vehicle to enter a guideway segment contrary to the current direction of travel. This vehicle would be stopped by provision 1 (one way safe tones) and would be protected from oncoming traffic by the safe tone ahead which would turn off due to the status of the block occupied by the vehicle.



The exchange technique for updating block occupancy generally gives the same results as the MPM technique. For example, slide-through protection is provided since both blocks are occupied before a slide-through occurs. Therefore, the exchange method leaves both blocks occupied (i.e., the departed block is not cleared). Two MPM features are not inherent but can be added.

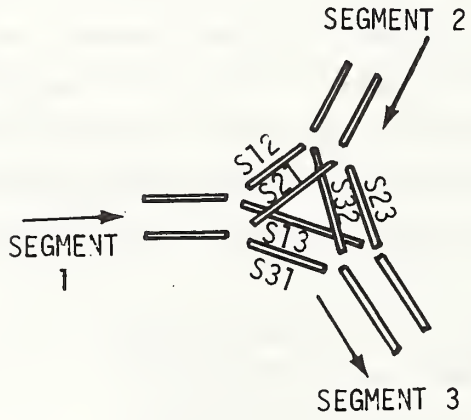
1. If the initial status is incorrect, a vehicle can be "discovered" since the block entered is unconditionally set occupied when a PD is activated.

2. False activation of the PD behind a vehicle will not clear the occupied block.

Both of the above conditions are very improbable but can be easily covered by unconditionally setting the block ahead occupied when a PD is activated. (The block "ahead" is determined by the current authorized travel direction.) This must be done after the block occupancy exchange.

3. Guarded Entry to Directional Segments

The guideway is divided into directional segments. Entry to each segment is guarded by safe tones controlled by the segment direction.

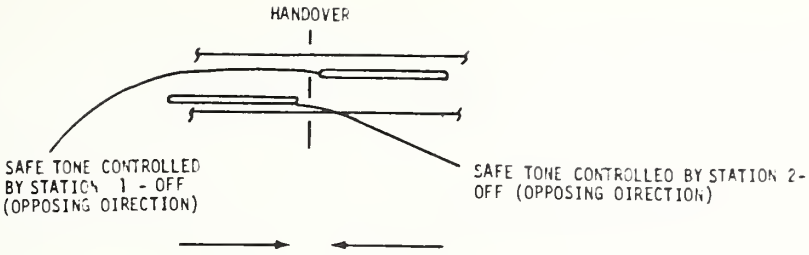


Safe tones S12 and S13 are off when segment 1 direction is normal. Thus, opposing traffic is prevented from either of the other segments. Similarly, safe tones S21 and S23 guard segment 2. S31 and S32 guard segment 3 when its direction is reversed.

This protection is a natural result of provision 1.

4. Guarded Entry at Handover

Entry to the guideway controlled by each station is guarded by a safe tone controlled by the station to be entered. Traffic cannot enter the station in a direction contrary to the direction specified by the station since the entry safe tone will be off per provision 1. Thus, a failure mode in which adjacent stations are set up with opposite directions (toward each other) will stop vehicles prior to handover in both directions.


HANDOVER
SAFE TONE CONTROLLED BY STATION 1 - OFF (OPPOSING DIRECTION)
SAFE TONE CONTROLLED BY STATION 2- OFF (OPPOSING DIRECTION)

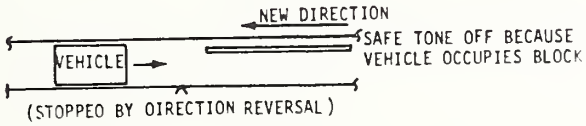
5. Direction Control

If the direction status for a given segment were to change inadvertently, vehicles would still be protected.

a. Vehicles traveling in the initial direction would be stopped by provision 1. (That direction is now off.)

b. Vehicles entering in the opposite direction would be stopped due to failure to recalculate safe tones for the reverse direction. (This is done only when a direction change is commanded.)

c. The safe tone ahead of each initial vehicle cannot be turned on for the new direction because the controlling block remains occupied due to provision 2.



A command to reverse direction is honored only if all blocks in the segment are clear. If the command is honored, safe tones are initialized to normal values for the new direction and turned off for the opposite direction. Otherwise all safe tones are turned off.

APPENDIX A - GLOSSARY

CAS	Collision Avoidance System
C&CS	Control and Communication System
CCCS	Central Control and Communication System
Downlink	Vehicle to wayside communication
DSU	Destination Selection Unit
ECU	Environment Control Unit
FMEA	Failure modes and effects analysis
FSK	Frequency Shift Keying
Headway	Time separation between successive vehicles
JPL	Jet Propulsion Laboratory, Pasadena, California
Loop	An inductive communication antenna extending along a length of guideway
MPM	Morgantown People Mover
PD	Presence Detection
RAM	Random access memory
ROM	Read only memory
SCCS	Station Control and Communication System

UMTA	Urban Mass Transportation Administration
Uplink	Wayside to vehicle communication
UPS	Uninterruptable power supply
VCCS	Vehicle Control and Communication System
WVU	West Virginia University

APPENDIX B - REPORT OF NEW TECHNOLOGY

This report, for the first time, pulls together information which will aid future designers of collision avoidance systems. Section 4 presents design considerations and the resulting design solutions. Section 5 evaluates the design and discusses problems encountered and their solutions. Section 6 provides design alternatives which might be considered for future collision avoidance systems.

☆ U. S. GOVERNMENT PRINTING OFFICE: 1980--700-271--209

DATE
1711-USMA
757 Jefferson

DOT LIBRARY
00009240